Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2016

195

Besluit van 17 mei 2016, houdende regels betreffende de verwerking van persoonsgegevens in de voorzieningen voor de generieke digitale infrastructuur DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister (Besluit verwerking persoonsgegevens generieke digitale infrastructuur)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties van 18 januari 2016, nr. 2016-0000023784 DCB/CZW/SB;

Gelet op artikel X, derde lid, van de Wet elektronisch berichtenverkeer Belastingdienst;

De Afdeling advisering van de Raad van State gehoord (advies van 8 april 2016, nr. No.W04.160008/I);

Gezien het nader rapport van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties van 10 mei 2016 nr. 2016-0000267641 BZK/CZW/SB;

Hebben goedgevonden en verstaan:

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1

In dit besluit wordt verstaan onder:

afnemer van DigiD en DigiD Machtigen: een overheidsorgaan dat, of een rechtspersoon met een wettelijke taak, niet zijnde een overheidsorgaan, die bij de uitoefening van zijn taak of bevoegdheid een dienst aanbiedt voor elektronisch verkeer tussen hem en gebruikers van DigiD respectievelijk DigiD Machtigen en daarbij gebruik maakt van DigiD respectievelijk DigiD Machtigen;

afnemer van MijnOverheid: een overheidsorgaan dat, of een rechtspersoon met een wettelijke taak, niet zijnde een overheidsorgaan, die bij de uitoefening van zijn taak of bevoegdheid gebruik maakt van MijnOverheid;

authenticatie: een elektronisch proces voor de verificatie en bevestiging van de identiteit van een natuurlijke persoon of rechtspersoon of van de oorsprong en integriteit van gegevens;

bezoeker van MijnOverheid, DigiD of DigiD Machtigen: degene die MijnOverheid, DigiD of DigiD Machtigen bezoekt, maar niet inlogt of van wie de elektronische aanvraagprocedure voor een DigiD niet is voltooid;

BSN-Koppelregister: de voorziening die een relatie legt tussen een uniek identificerend kenmerk op een privaat authenticatiemiddel en het burgerservicenummer van de houder;

burgerservicenummer: het nummer, bedoeld in artikel 1, onderdeel b, van de Wet algemene bepalingen burgerservicenummer;

DigiD: de voorziening voor uitgifte van elektronische authenticatiemiddelen en voor elektronische authenticatie die bereikbaar is via het webadres www.digid.nl;

DigiD Machtigen: de voorziening voor elektronische registratie van machtigingen die bereikbaar is via het webadres machtigen.digid.nl;

gebruiker van DigiD: een natuurlijk persoon die is ingeschreven in de basisregistratie personen, in het bezit is van een burgerservicenummer en van wie de elektronische aanvraagprocedure voor een DigiD is voltooid;

gebruiker van DigiD Machtigen: de gemachtigde, de vertegenwoordigde of een natuurlijke persoon of rechtspersoon, die gebruik maakt van de voorziening DigiD Machtigen;

gebruiker van MijnOverheid: een natuurlijk persoon die is ingeschreven in de basisregistratie personen, in het bezit is van een burgerservicenummer, en voor wie een MijnOverheid-account beschikbaar is;

gemachtigde: een gebruiker van DigiD Machtigen die namens de vertegenwoordigde bepaalde (rechts)handelingen kan verrichten;

gemachtigde in MijnOverheid: een gebruiker van MijnOverheid of een rechtspersoon, die met een in DigiD Machtigen geregistreerde machtiging in MijnOverheid bepaalde berichten van de vertegenwoordigde in kan zien;

MijnOverheid: de voorziening die bereikbaar is via het webadres mijn.overheid.nl voor de dienst voor elektronisch berichtenverkeer de Berichtenbox, en de diensten voor informatieverschaffing Lopende Zaken en Persoonlijke gegevens;

MijnOverheid-account: het domein van een gebruiker van MijnOverheid op MijnOverheid;

notificatie: een attendering die met een e-mailbericht of via een ander kanaal aan de gebruiker van MijnOverheid wordt verstuurd nadat een bericht in de Berichtenbox is geplaatst of een wijziging in Lopende Zaken heeft plaatsgevonden;

Onze Minister: Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties;

overheidsorgaan: overheidsorgaan als bedoeld in artikel 1, onderdeel c, van de Wet algemene bepalingen burgerservicenummer;

persoonsgegevens: hetgeen daaronder wordt verstaan in artikel 1 van de Wet bescherming persoonsgegevens;

vertegenwoordigde: een natuurlijk persoon die zich ter behartiging van zijn belangen in het verkeer met afnemers van DigiD Machtigen laat vertegenwoordigen door een gemachtigde;

vertegenwoordigde in MijnOverheid: een natuurlijk persoon die, met een in DigiD Machtigen geregistreerde machtiging, een gemachtigde in MijnOverheid toegang verleent tot zijn berichten voor zover deze vallen binnen de reikwijdte van de machtiging.

HOOFDSTUK 2. DE VERWERKING VAN PERSOONSGEGEVENS

Artikel 2 Persoonsgegevens DigiD

Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van DigiD de volgende persoonsgegevens:

a. over bezoekers van DigiD: gegevens over herkomst en kenmerken van het netwerkverkeer en de kenmerken van de gebruikte software en hardware van de bezoeker van DigiD die relevant zijn voor de adequate werking en beveiliging van de voorziening;

b. over bezoekers van DigiD die een aanvraagprocedure zijn gestart, maar niet hebben voltooid, tevens het burgerservicenummer en de datum en tijd van de aanvraag en de reden waarom de aanvraag niet is gelukt;

c. over gebruikers van DigiD:

1°. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum, de datum van overlijden, de nationaliteit, gegevens om het ingezetenschap of niet-ingezetenschap in de basisregistratie personen vast te kunnen stellen en het adres;

2°. een nummer dat ter identificatie van een persoon kan worden gebruikt, waaronder het burgerservicenummer, het nummer van een Nederlandse paspoort of van een Nederlandse identiteitskaart en gegevens met betrekking tot het paspoort of de identiteitskaart, zoals de geldigheidsdata;

3°. de accountgegevens, waaronder het mobiele telefoonnummer, het e-mailadres, de gebruikersnaam, het versleutelde wachtwoord, en overige gegevens die bij het account horen;

4°. de gebruiksgegevens, waaronder het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van DigiD is ingelogd, handelingen van de gebruiker, het door de gebruiker van DigiD gekozen authenticatieniveau, de website van de instelling waar de gebruiker van DigiD een DigiD aanvraagt of vanuit welke de gebruiker van DigiD met DigiD inlogt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik;

5°. gegevens die relevant zijn voor de adequate werking van de voorziening, waaronder in ieder geval de kenmerken van de door de gebruiker van DigiD gebruikte software en hardware.

6°. gegevens noodzakelijk voor de ondersteuning van de gebruiker, waaronder het burgerservicenummer en andere gegevens die worden verwerkt bij de ondersteuning van de gebruiker van DigiD.

Artikel 3 Persoonsgegevens DigiD Machtigen

Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van DigiD Machtigen de volgende persoonsgegevens:

a. over bezoekers van DigiD Machtigen: gegevens over herkomst en kenmerken van het netwerkverkeer en de kenmerken van de gebruikte software en hardware van de bezoeker van DigiD Machtigen die relevant zijn voor de adequate werking en beveiliging van de voorziening;

b. over gebruikers van DigiD Machtigen:

1°. de naam en de noodzakelijke gegevens om deze correct weer te geven, de datum van overlijden, het adres en van de vertegenwoordigde tevens de geboortedatum;

2°. het burgerservicenummer;

3°. gebruikersgegevens betreffende de machtigingsrelaties, inclusief de aanvragen daarvan, en profielgegevens;

4°. de gebruiksgegevens, waaronder gegevens over het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van DigiD Machtigen is ingelogd op de website van DigiD Machtigen, handelingen van de gebruiker van DigiD Machtigen (inloggen, aanvragen, intrekken en activeren), de afnemer van DigiD Machtigen waarvoor de gebruiker van DigiD Machtigen is gemachtigd, alsmede het tijdstip waarop dit gebeurt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik;

5°. gegevens die relevant zijn voor de adequate werking van de voorziening waaronder de kenmerken van de gebruikte software en hardware door de gebruiker van DigiD Machtigen;
6°. gegevens noodzakelijk voor de ondersteuning van de gebruiker, waaronder het burgerservicenummer en andere gegevens die worden verwerkt bij de ondersteuning van de gebruiker van DigiD Machtigen.

Artikel 4 Persoonsgegevens MijnOverheid

Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van MijnOverheid de volgende persoonsgegevens:
a. over bezoekers van MijnOverheid: gegevens over de herkomst en kenmerken van het netwerkverkeer en de kenmerken van de gebruikte software en hardware van de bezoeker van MijnOverheid die relevant zijn voor de adequate werking en beveiliging van de voorziening;
b. over gebruikers van MijnOverheid:
1°. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum, de datum van overlijden, de nationaliteit, gegevens om te bepalen of een natuurlijk persoon kwalificeert als gebruiker van MijnOverheid waarvoor de Berichtenbox beschikbaar moet kunnen zijn, en het adres;
2°. het burgerservicenummer,
3°. de accountgegevens, waaronder gegevens over het aanmaken en wijzigen van het MijnOverheid-account, het e-mailadres of ander kanaal waarop de gebruiker van MijnOverheid notificaties ontvangt, en gegevens over de verificatie daarvan, de schermnaam, en de door de gebruiker van MijnOverheid geselecteerde afnemer of afnemers van MijnOverheid ten aanzien van wie de gebruiker van MijnOverheid in de berichtenvoorkeuren van MijnOverheid kenbaar heeft gemaakt dat hij langs elektronische weg voldoende bereikbaar is voor het ontvangen van elektronische berichten in de Berichtenbox, meta-gegevens die horen bij berichten of zaaksgegevens, inloghistorie, en overige gegevens of wijzigingen daarvan die bij het account horen;
4°. de gebruiksgegevens, waaronder gegevens over de navigatie en handelingen van de gebruiker van MijnOverheid in de voorziening, inclusief het opvragen, tonen of wijzigen van gegevens of het falen van functies, gegevens over de verzending van notificaties en het eventueel falen daarvan, en overige gegevens met betrekking op het soort, tijdstip en kenmerken van het gebruik;
5°. gegevens die relevant zijn voor de adequate werking van de voorziening, waaronder sessie-cookies, gegevens over de herkomst en kenmerken van het netwerkverkeer en de kenmerken van de gebruikte software en hardware;
6°. gegevens noodzakelijk voor de ondersteuning van de gebruiker van MijnOverheid, waaronder het burgerservicenummer en andere gegevens die worden verwerkt bij de ondersteuning van de gebruiker;
c. over de vertegenwoordigde in MijnOverheid en de gemachtigde in MijnOverheid:
1°. de naam en de geboortedatum van de vertegenwoordigde in MijnOverheid en de noodzakelijke gegevens om deze correct weer te geven aan de gemachtigde in MijnOverheid;
2°. het burgerservicenummer van de vertegenwoordigde in MijnOverheid;
3°. de gebruiksgegevens, waaronder gegevens over de verzending van notificaties en het eventueel falen daarvan, gegevens over de handelingen van de gemachtigde in MijnOverheid ten aanzien van de gegevens van de vertegenwoordigde in MijnOverheid, waaronder begrepen het wijzigen van gegevens, inclusief gegevens over het falen van functies, en overige gegevens met betrekking tot het soort, tijdstip en kenmerken van het

gebruik;
4°. wijzigingen van meta-gegevens van het bericht of de berichten waarop de machtiging betrekking heeft.

Artikel 5 Persoonsgegevens BSN-Koppelregister

Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van het BSN-Koppelregister de volgende persoonsgegevens over de gebruiker van een privaat authenticatiemiddel, die dit middel wil gebruiken voor de afname van diensten van overheidsorganen en natuurlijke en rechtspersonen, niet zijnde overheidsorganen, die gerechtigd zijn het burgerservicenummer te gebruiken:
a. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum en de datum van overlijden;
b. het burgerservicenummer;
c. het uniek identificerende kenmerk op het private authenticatiemiddel;
d. de datum van registratie en eventuele deregistratie van de koppeling tussen het private authenticatiemiddel en het burgerservicenummer;
e. het tijdstip van inloggen bij de publieke dienstverlener.

HOOFDSTUK 3. DE VERSTREKKING VAN PERSOONSGEGEVENS

Artikel 6 Verstrekkingen in verband met DigiD

Onze Minister verstrekt aan de afnemers van DigiD:
a. het burgerservicenummer ten behoeve van de vaststelling van de identiteit van de gebruiker van DigiD;
b. het door de gebruiker van DigiD gekozen authenticatieniveau en het IP-adres.

Artikel 7 Verstrekkingen in verband met DigiD Machtigen

Onze Minister verstrekt op verzoek van afnemers van DigiD Machtigen:
a. een bewijs van geldigheid van een specifieke machtigingsregistratie voor diensten van de betreffende afnemer;
b. een overzicht van alle machtigingsaanvragen en machtigingsregistraties die voor diensten van de betreffende afnemer zijn afgegeven.

Artikel 8 Verstrekkingen in verband met MijnOverheid

Onze Minister verstrekt aan een afnemer van MijnOverheid:
a. het burgerservicenummer en, waar van toepassing, de status van de toepasselijke berichtenvoorkeur van de gebruiker van MijnOverheid, voorafgaand aan het aanleveren en ter bevestiging van het afleveren van berichten en gegevens, of het falen daarvan, ten behoeve van de werking van de diensten van MijnOverheid;
b. op verzoek van een afnemer die de Berichtenbox van MijnOverheid als verplicht kanaal voor elektronisch berichtenverkeer heeft aangewezen, informatie of een gebruiker van een MijnOverheid-account waarop de uitvoering van die taak betrekking heeft, zijn account wel of niet in gebruik heeft genomen en het bijbehorende burgerservicenummer.

Artikel 9 Verstrekkingen in verband met het BSN-Koppelregister

Onze Minister verstrekt het burgerservicenummer van de gebruiker van een privaat authenticatiemiddel, die dit middel wil gebruiken voor de afname van diensten door overheidsorganen en natuurlijke en rechtspersonen, niet zijnde overheidsorganen, die gerechtigd zijn het burgerser-

vicenummer te gebruiken in versleutelde vorm aan de bedoelde overheidsorganen en natuurlijke en rechtspersonen, niet zijnde overheidsorganen of degenen die namens hen optreden.

Artikel 10 Overige verstrekkingen

Onverminderd het bepaalde in de artikelen 6 tot en met 9, verstrekt Onze Minister geen gegevens over een bezoeker of gebruiker van DigiD, DigiD Machtigen of MijnOverheid aan anderen dan de bezoeker of de gebruiker zelf zonder voorafgaande toestemming van de bezoeker of de gebruiker, tenzij:

a. het een verstrekking betreft aan een overheidsorgaan of rechtspersoon met een wettelijke taak die noodzakelijk is voor de borging van de beveiliging en betrouwbaarheid van de betreffende voorziening, of

b. hij daartoe gerechtigd is op grond van een wettelijke bepaling.

HOOFDSTUK 4. DE BEWAARTERMIJN VAN PERSOONSGEGEVENS

Artikel 11 Bewaartermijnen in verband met DigiD

1. De gegevens over bezoekers van DigiD, bedoeld in artikel 2, onderdelen a en b, worden maximaal 18 maanden bewaard.

2. De naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum, de datum van overlijden, de nationaliteit, gegevens om het ingezetenschap of niet-ingezetenschap in de basisregistratie personen vast te kunnen stellen en het adres, bedoeld in artikel 2, onderdeel c, onder 1°, worden maximaal 6 weken bewaard.

3. De gebruiksgegevens, bedoeld in artikel 2, onderdeel c, onder 4°, worden maximaal 5 jaar bewaard, met dien verstande dat de sessiegegevens slechts worden bewaard tot het moment van uitloggen door de gebruiker.

4. Een nummer dat ter identificatie van een persoon kan worden gebruikt als bedoeld in artikel 2, onderdeel c, onder 2°, wordt bewaard:

a. gedurende het aanvraagproces maximaal 18 maanden, of;

b. zo lang het bijbehorende DigiD geldig is, en zodra dat niet meer het geval is maximaal 5 jaar.

5. De accountgegevens, bedoeld in artikel 2, onderdeel c, onder 3°, die nodig zijn voor het actuele gebruik van DigiD, zoals het actuele mobiele telefoonnummer en e-mailadres, de actuele gebruikersnaam, het actuele wachtwoord, het account-ID en de status van het account worden bewaard zo lang het bijbehorende DigiD geldig is, en zodra dat niet meer het geval is maximaal 5 jaar.

6. De overige accountgegevens, bedoeld in artikel 2, onderdeel c, onder 3°, worden maximaal 18 maanden bewaard.

7. De gegevens die relevant zijn voor de adequate werking van de voorziening, bedoeld in artikel 2, onderdeel c, onder 5°, worden bewaard zo lang de gebruiker van DigiD is ingelogd.

8. De gegevens noodzakelijk voor de ondersteuning van de gebruiker, bedoeld in artikel 2, onderdeel c, onder 6°, worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden.

Artikel 12 Bewaartermijnen in verband met DigiD Machtigen

1. De gegevens over bezoekers van DigiD Machtigen, bedoeld in artikel 3, onderdeel a, worden maximaal 18 maanden bewaard.

2. De naam en de noodzakelijke gegevens om deze correct weer te geven, de datum van overlijden, het adres en de geboortedatum, bedoeld in artikel 3, onderdeel b, onder 1°, worden maximaal 6 weken bewaard.

3. De gebruiksgegevens, bedoeld in artikel 3, onderdeel b, onder 4° en 5°, worden maximaal 5 jaar bewaard, met dien verstande dat de sessiegegevens slechts worden bewaard tot het moment van uitloggen door de gebruiker van DigiD Machtigen.

4. Het burgerservicenummer wordt bewaard zo lang de bijbehorende machtigingsaanvraag dan wel machtigingsregistratie niet is beëindigd, en zodra die wel is beëindigd maximaal 5 jaar.

5. De gebruikersgegevens, bedoeld in artikel 3, onderdeel b, onder 3°, worden bewaard zo lang machtigingsaanvraag dan wel machtigingsregistratie niet is beëindigd en zodra die wel is beëindigd maximaal 5 jaar.

6. De gegevens noodzakelijk voor de ondersteuning van de gebruiker, bedoeld in artikel 3, onderdeel b, onder 6°, worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden.

Artikel 13 Bewaartermijnen in verband met MijnOverheid

1. De gegevens over bezoekers van MijnOverheid, bedoeld in artikel 4, onderdeel a, worden maximaal 18 maanden bewaard.

2. De gegevens over gebruikers van MijnOverheid, bedoeld in bedoeld in artikel 4, onderdeel b, onder 4° en 5°, worden maximaal 5 jaar bewaard, met dien verstande dat sessie cookies slechts worden bewaard tot het moment van uitloggen.

3. De gegevens over een gebruiker van MijnOverheid en zijn MijnOverheid-account, bedoeld in artikel 4, onderdeel b, onder 1°, 2° en 3°, worden bewaard zolang het bijbehorende MijnOverheid-account bestaat, en zodra het account is opgeheven, maximaal 1 jaar, met uitzondering van de nationaliteit, de geboortedatum, de datum van overlijden en gegevens om te bepalen of een natuurlijk persoon kwalificeert als gebruiker van MijnOverheid waarvoor de Berichtenbox beschikbaar moet kunnen zijn, die bewaard blijven voor de duur van het aanmaak- of controleproces.

4. De gegevens noodzakelijk voor de ondersteuning van de gebruiker, bedoeld in artikel 4, onderdeel b, onder 6°, worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden.

5. De bewaartermijn van de gegevens over de vertegenwoordigde en de gemachtigde, bedoeld in artikel 4, onderdeel c, is als volgt:

a. de gegevens, bedoeld onder 1° en 2°, blijven bewaard tot het moment van uitloggen;

b. de gegevens, bedoeld onder 3°, blijven maximaal 5 jaar bewaard;

c. de gegevens, bedoeld onder 4°, blijven bewaard zo lang het MijnOverheid-account bestaat, en zodra dat account is opgeheven, maximaal 1 jaar.

6. Voor de gegevens, bedoeld in artikel 4, die zijn betrokken bij of relevant zijn voor het onderzoek naar een incident waarbij integriteit, vertrouwelijkheid of beschikbaarheid van het systeem in het geding is, wordt de in het eerste, derde en vierde, en vijfde lid, onderdeel c, genoemde bewaartermijn van 18 maanden of 1 jaar verlengd tot 36 maanden.

Artikel 14 Bewaartermijnen in verband met het BSN-Koppelregister

De bewaartermijn van de gegevens, bedoeld in artikel 5, is als volgt:

a. naam, geboortedatum en datum van overlijden worden niet langer bewaard dan nodig is om de gegevens op juistheid te controleren;

b. het burgerservicenummer wordt maximaal 18 maanden na registratie van de koppeling bewaard;

c. het uniek identificerende kenmerk op het private authenticatiemiddel wordt maximaal 18 maanden na de registratie van de koppeling bewaard;

d. de datum van registratie en eventuele deregistratie van de koppeling

wordt maximaal 18 maanden bewaard;
e. het tijdstip van inloggen bij de publieke dienstverlener wordt maximaal 18 maanden bewaard.

Artikel 15 Vernietiging na afloop bewaartermijn

Na het verstrijken van de bewaartermijn worden de gegevens zo spoedig mogelijk vernietigd.

HOOFDSTUK 5. SLOTBEPALINGEN

Artikel 16

Dit besluit treedt in werking met ingang van de dag na de datum van uitgifte van het Staatsblad waarin het wordt geplaatst en werkt terug tot en met 1 november 2015.

Artikel 17

Dit besluit wordt aangehaald als: Besluit verwerking persoonsgegevens generieke digitale infrastructuur.

Het advies van de Afdeling advisering van de Raad van State wordt met de daarbijbehorende stukken openbaar gemaakt door publicatie in de Staatscourant.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

Wassenaar, 17 mei 2016

Willem-Alexander

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk

Uitgegeven de *zevenentwintigste* mei 2016

De Minister van Veiligheid en Justitie,
G.A. van der Steur

stb-2016-195
ISSN 0920 - 2064
's-Gravenhage 2016

NOTA VAN TOELICHTING

Algemeen deel

1. Inleiding

De Wet elektronisch berichtenverkeer Belastingdienst (Wet EBV) biedt in artikel X een basis voor de voorzieningen voor «elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en elektronische registratie van machtigingen». Aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties (Minister van BZK) wordt de zorg voor deze voorzieningen opgedragen. Op dit moment gaat het om de voorzieningen DigiD, DigiD Machtigen, MijnOverheid en het BSN-Koppelregister. In artikel X is echter gekozen voor een generieke formulering, zodat ook eventuele andere voorzieningen voor de genoemde functies daaronder kunnen worden gebracht.

In dit besluit is nader bepaald welke persoonsgegevens ten behoeve van de «inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid» van deze voorzieningen worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. Omdat het hier gaat om de verwerking van het burgerservicenummer (hierna: BSN) en andere tot de burger herleidbare persoonsgegevens is een publiekrechtelijke grondslag door middel van een wettelijke verankering in de Wet EBV gecreëerd, aangevuld met een nadere uitwerking in dit besluit.

De voorziening MijnOverheid biedt via een website een persoonlijk domein aan burgers, voor zijn zaken met de overheid. MijnOverheid biedt momenteel drie diensten: de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens. De Berichtenbox is een persoonlijke, beveiligde elektronische postbus voor burgers. Met Lopende Zaken kan de status van bijvoorbeeld een vergunningaanvraag gevolgd worden. Persoonlijke Gegevens biedt inzicht in de eigen algemene gegevens die over de betreffende burger bekend zijn bij de overheid, bijvoorbeeld zoals opgenomen in basisregistraties.

Om toegang te krijgen tot MijnOverheid (en vele andere portalen van overheden en organisaties met een publiekrechtelijke taak), moet worden ingelogd met een voorziening voor elektronische authenticatie, thans is dit DigiD. Om ook ruimte te bieden aan private authenticatiemiddelen voor elektronisch zaken doen met de overheid, wordt momenteel gewerkt aan de totstandkoming van een eID-stelsel, waarbinnen publieke en private digitale authenticatiemiddelen naast elkaar kunnen functioneren (multi-middelen benadering). Om het mogelijk te maken dat burgers met private authenticatiemiddelen elektronische diensten in het publieke domein kunnen afnemen is de voorziening BSN-Koppelregister noodzakelijk. Dit BSN-Koppelregister is een publieke voorziening die een koppeling vastlegt tussen het unieke identificerende kenmerk op een privaat authenticatiemiddel (een zogenoemd pseudo-ID) en het burgerservicenummer van de houder. Door het inschakelen van het BSN-Koppelregister bij het inloggen bij een overheidsorganisatie of rechtspersoon met een wettelijke taak (publieke dienstverleners), krijgt deze organisatie het BSN van de houder meegeleverd. Dit is noodzakelijk omdat het BSN overheidsbreed als identificerend persoonsnummer wordt gebruikt.

Op de website van DigiD Machtigen kan een burger registreren dat hij een ander machtigt om zijn zaken met de overheid te regelen. Op deze voorziening voor de registratie van machtigingen zijn diensten van

verschillende overheidsorganisaties aangesloten, bijvoorbeeld voor het doen van aangifte inkomstenbelasting of het regelen van toeslagzaken.

De voorzieningen DigiD, DigiD Machtigen, MijnOverheid en het BSN-Koppelregister zijn in beheer bij Logius, de dienst digitale overheid die valt onder verantwoordelijkheid van de Minister van BZK.

Wat betreft de voorzieningen DigiD, DigiD Machtigen en MijnOverheid is in dit besluit grotendeels de bestaande praktijk van gegevensverwerking, bewaring en verstrekking van persoonsgegevens gecodificeerd. Het BSN-Koppelregister is nieuw.

Op basis van artikel X van de Wet EBV is tevens een ministeriële regeling tot stand gekomen met technische en administratieve voorschriften over de werking, beveiliging en betrouwbaarheid van de voorzieningen (Regeling voorzieningen GDI). Het gaat hierbij onder meer om zaken die eerder in de gebruiksvoorwaarden van DigiD, DigiD Machtigen en MijnOverheid waren opgenomen en om bestaande, in de praktijk gehanteerde voorschriften inzake informatieveiligheid. Ook wordt de functie en werking van de voorziening BSN-Koppelregister uitgewerkt.

Met de Wet EBV wordt de Berichtenbox van MijnOverheid aangewezen als verplicht kanaal voor berichten van de Belastingdienst. In paragraaf 8.2 van het algemeen deel van deze nota van toelichting, onder het kopje «Legitiem doel» wordt daaraan meer aandacht besteed.

Voor wat betreft het bredere kader waarbinnen het ontwerpbesluit gezien moet worden, moet worden opgemerkt dat er diverse – sectorspecifieke en generieke – wetsvoorstellen en bijbehorende uitvoeringsregels in verschillende stadia van voorbereiding zijn, die betere digitale dienstverlening door de overheid beogen. Het onderhavige besluit maakt deel uit van dat brede kader en dient zoals gesteld ter uitvoering van artikel X, derde lid, van de Wet EBV. Teneinde een juiste uitvoering van deze wet mogelijk te maken is in artikel X, eerst lid, de verantwoordelijkheid voor de generieke digitale infrastructuur (GDI), waar de voorziening MijnOverheid deel van uitmaakt, verankerd en opgedragen aan de Minister van BZK. De Wet EBV moet wordt voor wat betreft artikel X worden beschouwd als voorloper van de in voorbereiding zijnde Wet generieke digitale infrastructuur (Wet GDI), waarin de GDI in den brede, en dus niet langer als onderdeel van een sectorspecifieke wet, zal worden geregeld. Om bestuursorganen goed, betrouwbaar en veilig toe te rusten voor hun digitale taken, zal de Wet GDI hen verplichten om op GDI-voorzieningen aan te sluiten en deze ook daadwerkelijk te gebruiken. Het faciliteren van bestuursorganen houdt verband met afdeling 2.3 van de Algemene wet bestuursrecht (nieuw), waarin burgers, naast de schriftelijk weg, het recht krijgen op elektronisch communiceren met de overheid. Om dit recht te kunnen effectueren, moeten bestuursorganen hierop ingericht zijn; daartoe dient onder meer de GDI. Benadrukt moet worden, dat de overheid door de Awb noch de Wet GDI de verplichting opgelegd krijgt om digitaal met burgers te communiceren. Tot slot is in dit verband relevant, dat de toegang tot publieke dienstverlening in de lidstaten van de EU wordt beslagen door de eIDAS Verordening[1]. Deze behelst, naast regels voor het grensoverschrijdend gebruik van elektronische vertrouwensdiensten (bijvoorbeeld elektronische handtekeningen) de wederzijdse erkenning binnen de EU van hoog betrouwbare en voordien genotificeerde authenticatiemiddelen. De eisen aan (publiek en

[1] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L257).

privaat uitgegeven) authenticatiemiddelen zullen ingevolge de Wet GDI worden gesteld.

2. Algemene aandachtspunten

2.1. Aanduiding voorzieningen voor elektronische diensten

In artikel X van de Wet EBV worden de voorzieningen voor elektronische diensten functioneel omschreven, zodat het artikel ook de grondslag kan bieden voor eventuele opvolgers van de huidige voorzieningen en eventuele nieuwe voorzieningen. In dit besluit worden de huidige voorzieningen DigiD, DigiD Machtigen en MijnOverheid en de nieuwe voorziening BSN-Koppelregister met hun (bij het publiek bekende) naam aangeduid. Op het moment dat er nieuwe voorzieningen bij komen, zal dit besluit worden aangepast om ook voor die voorzieningen regels te stellen over de in het kader van die voorziening te verwerken gegevens, de bewaartermijnen en de verstrekkingen.

2.2. Doelen van de gegevensverwerking

In artikel X, derde lid, in samenhang met het eerste lid, van de Wet EBV is duidelijk beschreven dat het doel van de verwerking van de persoonsgegevens door de Minister van BZK gelegen is in de goede vervulling van zijn taak om te zorgen voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing (MijnOverheid) alsmede van voorzieningen voor elektronische authenticatie (DigiD en BSN-Koppelregister) en elektronische registratie van machtigingen (DigiD Machtigen).

Deze doelen bestrijken meerdere processen die ten aanzien van de genoemde voorzieningen te onderscheiden zijn. In totaal zijn vijf processen te onderscheiden bij de voorzieningen, namelijk:
– het proces van aanvraag en/of activering van de diensten van de voorzieningen,
– het daadwerkelijke gebruik van de diensten,
– het verstrekken van gegevens aan afnemers van de voorzieningen,
– het verwerken van gegevens in verband met het borgen van de beveiliging en betrouwbaarheid van de voorzieningen,
– het afhandelen van vragen en klachten van gebruikers.

Per proces zal worden ingegaan op de gegevens die in het kader van dat proces worden verwerkt. Daaruit blijkt het meer concrete doel van de verwerking van de diverse gegevens en daarmee wordt ook de bijbehorende bewaartermijn gemotiveerd.

3. De verwerking van gegevens in het kader van DigiD

3.1. De aanvraag en activering

Bij de (digitale) aanvraag van DigiD (bijvoorbeeld via www.digid.nl) door iemand die als ingezetene is ingeschreven in de basisregistratie personen (hierna: BRP), wordt van de aanvrager zijn BSN, geboortedatum, postcode en huisnummer gevraagd. Vanuit de BRP worden op basis van een autorisatiebesluit op grond van artikel 3.2 van de Wet basisregistratie personen gegevens verstrekt aan de Minister van BZK (in de praktijk Logius namens deze). Uit deze verstrekking worden het BSN, de geboortedatum, de postcode en het huisnummer gebruikt om de door de aanvrager opgegeven gegevens te controleren. Ook wordt op basis van gegevens uit de BRP bekeken of de betreffende persoon als ingezetene is ingeschreven in de BRP. Als de opgegeven informatie overeenstemt met

de informatie in de BRP, gaat de aanvraagprocedure verder door de aanvrager te vragen of hij een gebruikersnaam en wachtwoord wil kiezen. Het wachtwoord wordt zo snel mogelijk gehasht (dat wil zeggen zodanig versleuteld opgeslagen dat het gehashte wachtwoord niet te herleiden is tot het oorspronkelijke wachtwoord) en dus niet in zijn oorspronkelijke vorm opgeslagen of bewaard. Daarna wordt de aanvrager de optie geboden de wachtwoordherstelfunctie in te stellen en wordt hem gevraagd of hij gebruik wil maken van DigiD met extra sms-controle (of in de toekomst mogelijk een andere authenticatiemiddel). In die gevallen moet de gebruiker ook zijn e-mailadres en/of zijn mobiele telefoonnummer opgeven. Aan het eind van de aanvraag wordt de zogenaamde activeringscode per post verzonden aan de burger. Wanneer de burger deze brief heeft ontvangen en de activeringscode succesvol in DigiD heeft ingevoerd, kan hij DigiD gaan gebruiken.

Voor diegenen die als niet-ingezetene zijn ingeschreven in de BRP en beschikken over een BSN, verloopt de procedure anders. Het woonadres van deze personen is (doorgaans) niet in Nederland. Voor diegenen die in het buitenland wonen en klant zijn van de Sociale Verzekeringsbank (SVB) en AOW-pensioen ontvangen, kan online een DigiD worden aangevraagd via de website van de SVB. De brief met activeringscode wordt dan door Logius verzonden naar het adres zoals dat bij de SVB geregistreerd staat.

Voor de overige niet-ingezetenen in de BRP die een DigiD willen aanvragen, staat een andere procedure open, mits het gaat om mensen met de Nederlandse nationaliteit. Zij kunnen via internet een aanvraag doen voor DigiD en moeten daarbij hun BSN, geboortedatum, het nummer van hun Nederlandse paspoort of Nederlandse identiteitskaart (en de datum waarop de geldigheid van het document eindigt opgeven. Ook hier vindt controle plaats via de BRP, waarbij ook de nationaliteit wordt gecontroleerd en of iemand als niet-ingezetene is ingeschreven in de BRP. Verder zijn nodig een mobiel telefoonnummer waarop de betrokkene op het moment van aanvraag in Nederland (en later tijdens het gebruik van DigiD in het buitenland) sms-berichten kan ontvangen en een e-mailadres. Voor deze doelgroep is een DigiD met extra sms-controle standaard. Hiermee kan de gebruiker vanuit zijn woonplaats in het buitenland eenvoudig zijn wachtwoord herstellen. Na het doorlopen van de aanvraag ontvangt de aanvrager een baliecode per sms en per e-mail. Deze baliecode kan op vertoon van het Nederlandse paspoort of de Nederlandse identiteitskaart en opgeven van het BSN, aan een van de DigiD-balies worden ingewisseld voor een activeringscode waarmee de DigiD geactiveerd kan worden. Deze balies zijn gevestigd in op dit moment een vijftal gemeenten in Nederland en bij de Nederlandse ambassade in Parijs; uitbreiding van het aantal balies (in het buitenland) is voorzien.

De naam, adres (inclusief woonplaats), de geboortedatum, de nationaliteit en gegevens om het ingezetenschap of niet-ingezetenschap in de basisregistratie personen vast te kunnen stellen zijn dus enkel nodig in het aanvraagproces. Zodra redelijkerwijs kan worden aangenomen dat de activeringscode de geadresseerde heeft bereikt, is bewaring van de naam, het adres en de woonplaats niet meer nodig. Aangezien ook post wordt verzonden naar adressen in het buitenland, wordt veiligheidshalve voor deze gegevens een bewaartermijn van 6 weken aangehouden vanaf het moment van aanvraag (artikel 11, tweede lid).

De bewaartermijn is geformuleerd als een maximale bewaartermijn. Waar 6 weken niet noodzakelijk is voor het doel waarvoor het gegeven wordt gebruikt, zal bewaring eerder worden beëindigd. Dat is bijvoorbeeld het geval bij de geboortedatum, de datum van overlijden, de nationaliteit en gegevens om het ingezetenschap of niet-ingezetenschap in de

basisregistratie personen vast te kunnen stellen; zodra die gegevens aan de hand van de gegevens uit de BRP zijn gecontroleerd, worden ze niet langer bewaard. Ook bij de balieprocedure geldt een kortere termijn: aangezien de verzonden baliecode binnen 30 dagen aan de balie moet worden omgewisseld in een activeringscode, is na die termijn bewaring van de naam en geboortedatum niet meer nodig.

Gegevens over het paspoort of de identiteitskaart (zoals nummer en geldigheid) zoals opgegeven bij de aanvraag en zoals gecontroleerd aan de balie worden bewaard tot het balie-uitgifteproces van het DigiD door de baliemedewerkers is gecontroleerd, met een maximum van 18 maanden om eventuele achterstand in controles op te kunnen vangen (artikel 11, vierde lid, onderdeel a). Voor de overige accountgegevens die in het balieproces worden verwerkt, zoals de datum en tijdstip van uitgifte van de activeringscode geldt een bewaartermijn van 18 maanden (artikel 11, zesde lid).

De activeringscode blijft 21 dagen geldig, met uitzondering van de aanvragen die via de SVB lopen en waarvoor de activeringscode naar het buitenland wordt verstuurd. Hiervoor geldt dat de activeringscode 45 dagen geldig blijft. Binnen deze periode dient de account geactiveerd te worden. Als de gebruiker dit niet doet, worden datum en tijd van de aanvraag (gebruiksgegevens als bedoeld in artikel 2, onderdeel c, onder 4°), het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van DigiD is ingelogd, en het BSN (de zogenaamde transactielogging) worden nog maximaal 5 jaar bewaard (artikel 11, derde lid). Ook hier is sprake van een maximumtermijn: d overige gebruiksgegevens die bij de aanvraag zijn verwerkt, zoals de gekozen gebruikersnaam, het e-mail adres en het telefoonnummer, worden na verloop van de activeringscode verwijderd.

Als de aanvraag van een DigiD om welke reden dan ook niet afgerond wordt en de bezoeker dus geen gebruiker wordt, worden de volgende gegevens gedurende 18 maanden bewaard (artikel 11, eerste lid): de datum en tijd van de aanvraag, gegevens over herkomst en kenmerken van het netwerkverkeer en de kenmerken van de gebruikte software en hardware van de bezoeker die relevant zijn voor de adequate werking van de voorziening en de reden waarom de aanvraag niet gelukt is. De reden kan bijvoorbeeld een mismatch met de gegevens in de BRP zijn of annuleren door de bezoeker zelf.

Het BSN, het e-mailadres en het mobiele telefoonnummer zijn niet alleen nodig bij de aanvraagprocedure, maar ook tijdens het gebruik van DigiD; op de bewaartermijn daarvan wordt hieronder ingegaan in de paragraaf 3.2 over gebruik.

3.2. Het gebruik

Zodra de aanvrager zijn DigiD heeft geactiveerd, kan hij het gebruiken om in te loggen bij diverse afnemers. Gegevens die in dat proces worden gebruikt zijn het BSN, de gebruikersnaam en het wachtwoord voor het vaststellen van de identiteit bij het inloggen door de Minister van BZK/ Logius en de afnemer. Bij het inloggen voert de gebruiker zelf zijn gebruikersnaam en wachtwoord in. Indien de gebruiker voor extra controle via sms heeft gekozen, of wanneer de afnemer controle via sms verplicht stelt, stuurt DigiD een code naar de mobiele telefoon van de gebruiker. Deze code dient de gebruiker vervolgens in te voeren in het inlogscherm.

Ter verhoging van het gebruikersgemak, kunnen afnemers «eenmalig inloggen» aanbieden. Met eenmalig inloggen hoeven gebruikers niet opnieuw in te loggen als ze in dezelfde browsersessie navigeren naar een andere website die ook eenmalig inloggen gebruikt (een burger die bijvoorbeeld is ingelogd op MijnOverheid hoeft dan niet opnieuw in te loggen als hij de berichten van de Belastingdienst in de Berichtenbox van MijnOverheid wil bekijken). Bij de Functionaliteit Eenmalig inloggen biedt Logius aan aangesloten afnemers zekerheid over de identiteit van een gebruiker, gedurende een sessie en gedurende een bepaalde periode nadat deze zich heeft geauthenticeerd bij DigiD, ook als gebruikers meerdere diensten van meerdere afnemers achter elkaar willen afnemen. In verband met deze dienst worden geen aanvullende persoonsgegevens verwerkt.

Allerlei aan het gebruik gerelateerde gegevens worden gedurende een inlogsessie verwerkt, zoals het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker inlogt, handelingen van de gebruiker (zoals het wijzigen van het wachtwoord), de website van de instelling waar de gebruiker van DigiD aanvraagt of van waaruit de gebruiker van DigiD met DigiD inlogt, het tijdstip van begin en einde van de inlogsessie en sessiecookies (artikel 2, onderdeel c, onder 4°). De bewaartermijn van deze gegevens is maximaal 5 jaar (artikel 11, derde lid); op de motivering daarvoor wordt uitgebreid ingegaan in hoofdstuk 6 van deze nota van toelichting.

Daarnaast zijn er de zogenaamde accountgegevens, waaronder de al genoemde gebruikersnaam en het wachtwoord, de status van het account (aangevraagd, geactiveerd, opgeschort of geblokkeerd), het actuele en eventueel eerder gebruikte mobiele telefoonnummer en e-mailadres, datum einde geldigheid van het account en het account-ID (artikel 2, onderdeel c, onder 3°). Deze gegevens zijn nodig om het gebruik van DigiD mogelijk te maken en eventuele vragen achteraf te beantwoorden.

Het BSN en (van de accountgegevens) het actuele mobiele nummer, het actuele e-mailadres, de gebruikersnaam, het gehashte wachtwoord, het account-ID en de status daarvan worden bewaard zolang het bijbehorende DigiD geldig is. Zodra het DigiD niet meer geldig is (zie daarvoor de Regeling voorzieningen GDI op grond van artikel X, tweede lid, van de Wet EBV), worden deze gegevens nog gedurende 5 jaar bewaard (artikel 11, vierde lid, onderdeel b, en vijfde lid). Ook deze bewaartermijn is een maximumtermijn; het wachtwoord wordt immers ogenblikkelijk gehasht en dus niet ongehasht bewaard.

De overige accountgegevens worden maximaal 18 maanden bewaard, ook als het bijbehorende DigiD daarna nog geldig is (artikel 11, zesde lid).

De bewaartermijn van de gegevens die relevant zijn voor de adequate werking van voorziening, de kenmerken van de gebruikte software en hardware door de gebruiker of de bezoeker, worden bewaard zo lang de gebruiker wel is ingelogd (artikel 11, zevende lid).

3.3 De verstrekking van gegevens

Na authenticatie van de gebruiker worden vanuit DigiD het BSN, het authenticatieniveau en het IP-adres van de gebruiker aan de afnemer verstrekt. Het BSN wordt verstrekt zodat de afnemer kan nagaan welke burger heeft ingelogd. Het authenticatieniveau wordt verstrekt zodat de afnemer een beeld heeft van de mate waarin er zekerheid is over de identiteit van de gebruiker die heeft ingelogd: een door de gebruiker gekozen hoger authenticatieniveau geeft meer zekerheid. Het IP-adres

wordt meegegeven zodat de afnemer het kan gebruiken om de gebruiker al dan niet toegang te verlenen.

4. De verwerking van gegevens in het kader van DigiD Machtigen

4.1. De aanvraag en activering

In DigiD Machtigen kan een machtiging voor een specifieke dienst worden geregistreerd als iemand een ander wil machtigen om zijn zaken met de overheid (digitaal) te regelen. Het registratieproces is opgedeeld in twee stappen, het aanvragen, gevolgd door het activeren van een machtigingsrelatie met behulp van een machtigingscode. De registratie kan ook zonder machtigingscode worden uitgevoerd mits er op voorhand zekerheid is dat de vertegenwoordigde en de gemachtigde de registratie willen.

Aanvragen

Een registratie van een machtiging kan in beginsel door iedere burger worden gedaan, en wel als vertegenwoordigde, beoogd gemachtigde of derde. Een aanvraag kan ook worden gedaan door organisaties die als gemachtigde willen optreden en door afnemers. Bij de aanvraag is in alle gevallen het BSN van vertegenwoordigde nodig en moet aangegeven worden voor welke diensten de registratie van de machtiging wordt gevraagd.

Aanvragen kunnen allereerst worden gedaan via de website van DigiD Machtigen. Er zijn ook organisaties die fungeren als gemachtigden, afnemers en helpdesks van afnemers die op de voorziening DigiD Machtigen zijn aangesloten. Aanvragen kunnen ook door hen (met behulp van eHerkenning[2]) of via hun voorzieningen worden gedaan. Een burger die een aanvraag doet via de website van DigiD Machtigen of de website van een afnemer zal op dat moment ingelogd zijn met zijn DigiD.

Bij een succesvolle aanvraag stuurt DigiD Machtigen kennisgevingen van de aangevraagde machtigingen met machtigingscodes per post naar de vertegenwoordigden. Er wordt geen kennisgeving verstuurd indien vertegenwoordigde zelf via de website de aanvraag heeft gedaan, in dit geval wordt de machtigingscode op de website getoond. Een kennisgeving wordt ook niet verstuurd in de gevallen waarin zowel vertegenwoordigde als gemachtigde in een zelfde sessie zijn ingelogd op een website die de functionaliteit «registratie zonder machtigingscode» ondersteunt (zie verder hieronder bij «activering»).

Een afnemer kan machtigingen ook aanvragen door een lijst met BSN's van vertegenwoordigden op te geven aan DigiD Machtigen. DigiD Machtigen verwerkt deze lijst tot aanvragen en stuurt een kennisgeving van de aanvraag aan de vertegenwoordigde, die vervolgens de machtigingscode kan overhandigen aan zijn gemachtigde (bijvoorbeeld een medewerker van de Hulp bij Aangifte voor de Inkomstenbelasting).

Activeren

Na de aanvraag dient de geregistreerde machtiging geactiveerd te worden. De vertegenwoordigde overhandigt de machtigingscode samen met zijn BSN aan de beoogd gemachtigde (een burger of medewerker van

---

[2] Op het moment van totstandkoming van dit besluit is inloggen met eHerkenning alleen mogelijk voor (medewerkers van) de Belastingdienst. De inspanningen zijn er op gericht dit vanaf eind 2016 mogelijk te maken voor alle afnemers die gebruik maken van DigiD Machtigen.

een organisatie) die daarmee de geregistreerde machtiging kan activeren en accepteren.

Het activeren kan via de website van DigiD Machtigen. Activering is ook mogelijk via afnemers die deze functionaliteit bieden.

Registratie zonder machtigingscode

Het registratieproces van een machtiging kan zonder tussenkomst of overdracht van een machtigingscode plaatsvinden als zowel vertegenwoordigde als gemachtigde in een zelfde sessie zijn ingelogd op een website die deze functionaliteit ondersteunt. De vertegenwoordiger logt in met DigiD bij een dienstaanbieder en doet een aanvraag. De gemachtigde dient direct daarna op dezelfde website in te loggen om de aanvraag te activeren.

Een machtigingscode wordt ook niet overgedragen bij de in ontwikkeling zijnde nabestaandenmachtiging. De aanvraag zal in dit geval door de afnemer worden gedaan, die via een formulier van de erven heeft doorgekregen wie als gemachtigde van de erven zal optreden. De gemachtigde kan nadat de aanvraag door de afnemer is gedaan, de nabestaandenmachtiging direct via de website activeren.

Persoonsgegevens

Bij het inloggen, aanvragen en activeren worden met de BSN's van aanvrager, vertegenwoordigde of gemachtigde gegevens uit de BRP verkregen, de naamgegevens worden gebruikt voor het tonen op de website, de geboortedatum en de status van de persoonslijst in de BRP worden gebruikt bij het controleren, en de namen en adresseringsgegevens worden gebruikt voor het sturen van kennisgevingen. Ook de datum van overlijden wordt indien van toepassing vanuit de BRP versterkt ter controle.

Bij een aanvraag door de gemachtigde of een andere aanvrager is de geboortedatum van de vertegenwoordigde nodig om ongewenste aanvragen te voorkomen. Het BSN van de aanvrager wordt bij de aanvraag geregistreerd. De aanvrager kan op verzoek en met instemming van de Helpdesk de aanvraag ook anoniem doen, zonder aangeven van zijn BSN. Het BSN van de aanvrager die niet anoniem de aanvraag doet, wordt bewaard zo lang de machtigingsrelatie niet is beëindigd en na beëindiging nog 5 jaar (artikel 12, vierde lid).

Gelet op het voorgaande proces is het bewaren van de naam, het adres en de geboortedatum na het aanvraagproces niet meer nodig. De bewaartermijn is daarom gesteld om maximaal 6 weken (artikel 12, tweede lid). Het BSN is ook nodig in het gebruiksproces; zie verder de toelichting bij artikel 11.

Ten slotte blijven de gegevens van het besturingssysteem en browsertype («user-agent») van een bezoeker, samen met het IP-adres, 18 maanden bewaard voor bezoekersstatistieken, trendanalyse, usability-onderzoek, klachtbehandeling en analyse van (beveiligings)incidenten (artikel 12, eerste lid). De 18 maanden termijn is gebaseerd op de tijdsduur die benodigd is voor adequate analyse en onderzoek alsmede de lengte van het klachtrecht van hoofdstuk 9 van de Awb.

4.2. Het gebruik en de verstrekking van gegevens

Op het moment dat een gemachtigde inlogt bij een afnemer en zaken wil regelen voor de vertegenwoordigde, worden het BSN van de vertegenwoordigde en de gemachtigde en de dienst verstrekt aan DigiD Machtigen. Op basis van beide BSN's en de dienst kan DigiD Machtigen controleren of de machtigingsrelatie geregistreerd is. Vanuit DigiD Machtigen wordt dan gemeld of de machtingsrelatie voor die dienst geregistreerd is of niet. Dit bewijs van de machtigingsrelatie bevat de identificatie van de dienstaanbieder, om welke dienst het gaat en het BSN van de vertegenwoordigde, het BSN van de gemachtigde (tenzij de gemachtigde geen natuurlijk persoon is) en het tijdstip van controle van de geldigheid van de machtiging (artikel 7, onderdeel a). De afnemers van DigiD Machtigen kunnen voorts een persoonsgericht overzicht opvragen van de machtigingsaanvragen en – registraties die voor diensten van de betreffende afnemer zijn afgegeven (artikel 7, onderdeel b). De reden daarvoor is serviceverlening aan de afnemers en gemachtigde.

5. De verwerking van gegevens in het kader van MijnOverheid

5.1. Algemeen

De voorziening MijnOverheid bevat drie diensten, namelijk de Berichtenbox, Lopende Zaken en Persoonlijke gegevens. Er wordt één account aangemaakt dat al deze drie diensten omvat. Deze drie diensten worden mogelijk in de toekomst uitgebreid met nieuwe, vergelijkbare diensten.

De Berichtenbox is een persoonlijke, beveiligde postbus voor digitale berichten van de overheid en rechtspersonen met een wettelijke taak. In de Berichtenbox kan de gebruiker berichten ontvangen, bewaren en beheren. De gebruiker kan zelf aangeven van welke overheidsorganisaties hij berichten wil ontvangen. Deze keuzemogelijkheid is er niet ten aanzien van de overheidsorganisaties waarvoor de Berichtenbox is aangewezen als verplicht kanaal voor elektronisch berichtenverkeer. Als er een nieuw bericht in de Berichtenbox is aangekomen, verstuurt MijnOverheid hierover een notificatie, mits de gebruiker aan heeft gegeven een dergelijk notificatiebericht te willen ontvangen en hiervoor een digitaal adres heeft opgegeven. Op dit moment wordt voor het versturen van notificaties e-mail gebruikt. Deze verzending vindt pas plaats nadat de gebruiker de geldigheid van het door hem opgegeven digitale adres heeft bevestigd door middel van een verzonden verificatiecode.

Een gebruiker van MijnOverheid kan ook iemand (of een rechtspersoon[3]) machtigen om zijn zaken met de overheid elektronisch te behartigen, door een machtiging(srelatie) te registreren in DigiD Machtigen. Zo kan een gemachtigde, onder een aparte tab in zijn eigen berichtenbox, inzage krijgen in één of meerdere berichten in de Berichtenbox van de vertegenwoordigde.

De dienst Lopende zaken informeert de gebruiker over zaken die hij bij de overheid heeft lopen, zoals een vergunningaanvraag. Lopende zaken geeft een overzicht van de lopende en afgeronde zaken met de overheid. De gebruiker ontvangt automatisch, per e-mail indien hij eerder een e-mailadres heeft opgegeven en bevestigd, een notificatie als er een wijziging in één of meer zaken is.

---

[3] De inspanningen zijn er op gericht deze mogelijkheid eind 2016 gerealiseerd te laten zijn.

Via de dienst Persoonlijke Gegevens kan de gebruiker zien hoe hij geregistreerd is bij de overheid. Het gaat daarbij om algemene gegevens die de overheid over hem heeft geregistreerd en gebruikt voor verschillende diensten. Zo heeft hij onder andere inzage in gegevens uit de BRP (o.a. woonadres, geboorte, verhuizing, huwelijk, kinderen), gegevens over zijn voertuig (RDW), perceelgegevens van zijn huis (Kadaster) en de waarderingsgegevens van zijn huis (WOZ).

Benadrukt wordt dat de Minister van BZK geen zeggenschap heeft over de inhoud van berichten in de Berichtenbox, zaaksgegevens in Lopende Zaken en gegevens in Persoonlijke Gegevens; daarover gaat de afnemer die de betreffende dienst van de Minister van BZK afneemt. De Minister van BZK fungeert wat de inhoud betreft als bewerker voor en onder verantwoordelijkheid van de betreffende afnemer. De inhoud van berichten in de Berichtenbox, zaaksgegevens in Lopende Zaken en gegevens in Persoonlijke Gegevens maken dus geen onderdeel uit van dit besluit, omdat de verwerking niet plaatsvindt in het kader van de zorgtaak van de Minister van BZK zoals geformuleerd in artikel X van de Wet EBV, maar op grond van de wettelijke taak van het bestuursorgaan dat afnemer is van MijnOverheid en dat verantwoordelijke is voor deze gegevens in de zin van de Wet bescherming persoonsgegevens.

5.2. Weergeven van de website

Iedere website (vergelijk ook paragraaf 4.1, laatste alinea, van deze nota van toelichting), en MijnOverheid is daarop geen uitzondering, herkent van iedere bezoeker en gebruiker het besturingssysteem en browsertype om de website passend weer te geven op diens toestel, computer of tablet. Samen met het IP-adres blijven de gegevens van het besturingssysteem en browsertype («user-agent») van een bezoeker 18 maanden bewaard voor bezoekersstatistieken, trendanalyse, usabilityonderzoek, klachtbehandeling en analyse van (beveiligings)incidenten (artikel 13, eerste lid). De 18 maanden termijn is gebaseerd op de tijdsduur die benodigd is voor adequate analyse en onderzoek alsmede de lengte van het klachtrecht van hoofdstuk 9 van de Awb. Voor de analyse van (beveiligings)incidenten hangt het verder af van de ernst of de 18 maanden termijn volstaat, dan wel dat deze termijn nogmaals moet worden verlengd met 18 maanden. Dit aan de hand van «best practices» in informatiebeveiliging (zie ook in paragraaf 5.7). Deze termijnen zijn adequaat als het gaat om gegevens over bezoekers. Bij gebruikers vallen deze gegevens onder de «gebruiksgegevens» die 5 jaar worden bewaard (artikel 13, tweede lid). Het waarborgen van de betrouwbaarheid van de voorziening ligt daar voornamelijk aan ten grondslag. In hoofdstuk 6 worden de zowel de redenen voor de bewaartermijn van 18 maanden als van 5 jaar verder uiteengezet.

5.3. Aanmaken van een account

MijnOverheid maakt deel uit van de GDI van de overheid. De Minister van BZK heeft de zorg voor deze GDI; daarvoor wordt wetgeving voorbereid. Gelet op de functie van MijnOverheid als generieke voorziening voor het realiseren van het recht op elektronisch zakendoen zoals neergelegd in het regeerakkoord van het kabinet Rutte II, ligt het in de rede dat voor alle burgers die redelijkerwijs zaken doen met de overheid een MijnOverheid-account beschikbaar moet zijn. Aangezien met name Nederlanders in het buitenland veel profijt kunnen hebben van deze elektronische dienstverlening wordt deze specifieke groep burgers daaronder mede begrepen. De doelgroep is daarmee bepaald tot alle burgers in Nederland (ingezetenen) en Nederlanders in het buitenland (niet-ingezetenen) van 14 jaar en ouder. Met het oog hierop, en mede ter

ondersteuning van het verplicht digitale verkeer met de Belastingdienst, is in de Wet EBV – vooruitlopend op de Wet generieke digitale infrastructuur (Wet GDI) – een grondslag opgenomen voor het aanmaken van deze MijnOverheidaccounts. Burgers voor wie een account is aangemaakt kunnen direct inloggen met hun DigiD en hun account personaliseren.

Om te bepalen of een MijnOverheid-account ambtshalve aangemaakt of op termijn weer opgeheven moet worden, dit laatste bijvoorbeeld na overlijden of als een gebruiker langdurig niet meer voldoet aan de criteria, worden gegevens ter controle opgevraagd uit de BRP en verwerkt door MijnOverheid. Daarnaast is het voor de omslag naar de nieuwe werkwijze onder de Wet EBV noodzakelijk om bestaande MijnOverheid-accounts, die in voorgaande jaren op verzoek van burgers zijn aangemaakt of op basis van de klantenadministratie van de Belastingdienst in rudimentaire vorm zijn klaargezet, te controleren en onderhouden aan de hand van gegevens uit de BRP. Hiervoor worden gegevens als BSN, nationaliteit, geboortedatum, datum overlijden en andere gegevens om te bepalen of een natuurlijk persoon kwalificeert als gebruiker van MijnOverheid waarvoor de Berichtenbox beschikbaar moet kunnen zijn opgevraagd en verwerkt voor de duur van het aanmaakproces of controleproces (artikel 13, derde lid). Het BSN van de gebruiker blijft wel verbonden aan het account zolang dit bestaat. Om de eerste stap naar het personaliseren van een account technisch in goede banen te leiden, wordt de naam van de gebruiker, inclusief alle noodzakelijke gegevens om deze juist te kunnen weergeven (zoals adellijke titel en predicaat en geslachtsnaam), opgevraagd en vooraf aan het account gekoppeld.

5.4. Personaliseren van een account

Na de eerste keer inloggen op MijnOverheid volgt het personaliseren van het account, deels automatisch, deels door de gebruiker zelf. De uit de BRP verkregen naam, inclusief alle noodzakelijke gegevens om deze juist te kunnen weergeven (zoals adellijke titel en predicaat en geslachtsnaam), wordt ter verificatie weergegeven aan de nieuwe gebruiker. Deze naam wordt vanaf dat moment bovenaan het scherm weergegeven, opdat de gebruiker weet dat hij is ingelogd in MijnOverheid. Ook wordt de gebruiker tijdens dit proces gevraagd om zijn e-mailadres op te geven als hij notificaties per e-mail wil ontvangen als er een nieuw bericht in zijn Berichtenbox is of een wijziging in zijn zaaksgegevens in Lopende Zaken heeft plaatsgevonden. Met een per e-mail toegezonden verificatiecode of door middel van een andere veilige en betrouwbare (toekomstige) techniek kan de gebruiker de werking van het opgegeven e-mailadres bevestigen. In de toekomst kan een gebruiker naast het e-mailadres waarschijnlijk ook kiezen voor andere notificatiekanalen.

Tenslotte wordt de gebruiker gevraagd of hij elektronisch bereikbaar wil zijn voor alle andere afnemers, uitgezonderd de Belastingdienst (de elektronische bereikbaarheid voor de Belastingdienst is een gegeven onder de Wet EBV). Deze keuze wordt na het eerste keer inloggen geboden en kan vervolgens te allen tijde worden aangepast door de gebruiker in de «berichtvoorkeuren» door de gewenste afnemers aan te vinken en andere uit. De naam en deze accountgegevens (zoals aanmaakdatum, wijzigingsdatum, e-mailadres, berichtvoorkeuren) blijven opgeslagen voor zolang als het account bestaat. Bij het wijzigen van deze gegevens, zoals het opgeven van een alternatief e-mailadres, blijft de originele invoer ook bewaard ten behoeve van gebruikersondersteuning, het waarborgen van de betrouwbaarheid en voor foutanalyse.

Omdat berichten lang beschikbaar moeten blijven in de Berichtenbox – tot een gebruiker ze verwijdert – en meta-gegevens (wanneer is het bericht geplaatst, gelezen, verplaatst, verwijderd) daaraan gerelateerd zijn, vallen ook deze gegevens onder accountgegevens en blijven bewaard

voor zolang het MijnOverheid-account bestaat (artikel 13, derde lid). Wanneer een gebruiker in zijn capaciteit als gemachtigde een handeling verricht met een bericht van een vertegenwoordigde (bijvoorbeeld verwijderen) dan wordt een wijziging van de meta-gegevens bij een bericht opgeslagen in het account van de vertegenwoordigde (artikel 13, vijfde lid, onderdeel c). Omdat een MijnOverheid-account nadrukkelijk het persoonlijk domein van de burger betreft wordt bijvoorbeeld het (meta)gegeven dat ervoor zorgt dat een bericht in de Berichtenbox als «gelezen» wordt weergegeven, uitsluitend verwerkt voor de goede werking van MijnOverheid.

Aangezien met het plaatsen van een bericht in de Berichtenbox het bericht geacht wordt te zijn ontvangen, is een periodieke controle op een geldig e-mailadres waaraan de notificatie is verzonden van groot belang voor de burgers zelf. Daarvoor wordt de inloghistorie bewaard en zo nodig het adres van de gebruiker opgevraagd uit de BRP om hem eventueel te wijzen op het belang van het in gebruik nemen en bereikbaar zijn via zijn MijnOverheid account.

5.5. Het gebruik

Iedere keer als een gebruiker inlogt met DigiD op MijnOverheid wordt ter beveiliging en alleen voor de duur van de sessie, een sessie-cookie met BSN verwerkt. Gedurende het gebruik van MijnOverheid worden over de gebruiker naast eerder genoemde accountgegevens, ook gebruiksgegevens («logging») over de handelingen en navigatie van de gebruiker in zijn MijnOverheid-account vastgelegd en tevens gegevens die relevant zijn voor de adequate werking van de voorziening (waaronder sessie-cookies, gegevens over de herkomst en kenmerken van het netwerkverkeer en de kenmerken van de gebruikte software en hardware)(artikel 4, onderdeel b, onder 4°). Deze gebruiksgegevens en gegevens met betrekking tot de adequate werking van de voorziening blijven maximaal 5 jaar bewaard (artikel 13, tweede lid, zie verder hoofdstuk 6). Gegevens over de verzending van e-mailnotificaties en het eventueel falen daarvan worden begrepen onder de gebruiksgegevens.

De additionele verwerking van gegevens als er sprake is van een elektronische machtiging, is omwille van de duidelijkheid apart beschreven in het besluit (artikel 4, onderdeel c). Een gemachtigde heeft vanuit zijn eigen MijnOverheid-account, maar achter een aparte tab, inzage in de berichten van een vertegenwoordigde die horen bij de specifieke machtiging. De controle van de geldigheid van de machtiging verloopt via een bevraging van DigiD Machtigen. Aangezien de communicatie met DigiD Machtigen uitsluitend verloopt via BSN, wordt voor de herkenbaarheid de naam en de geboortedatum van de vertegenwoordigde opgevraagd uit de BRP en weergegeven in het account van de gemachtigde. Vooral als een gemachtigde meerdere belanghebbenden vertegenwoordigt, is dit essentieel om de herkenbaarheid van de verschillende personen te kunnen borgen.

5.6. De verstrekking van gegevens

Voor de aflevering van een bericht in de Berichtenbox is het in beginsel voldoende als de verzendende afnemer kan aantonen of de geadresseerde kenbaar heeft gemaakt dat hij langs deze weg (MijnOverheid, Berichtenbox) voldoende bereikbaar is en het bericht ook daadwerkelijk daarin is afgeleverd. Voor het berichtenverkeer met de Belastingdienst is ingevolge de Wet EBV alleen het laatste aspect relevant, aangezien de berichtenvoorkeur niet op «uit» gezet kan worden.

Afnemers die de Berichtenbox niet als verplicht kanaal hebben aangewezen, controleren voorafgaand aan plaatsing van een bericht in een Berichtenbox aan de hand van het BSN bij het te verzenden bericht, of de betreffende Berichtenbox bestaat en de betreffende gebruiker de berichtenvoorkeur bij deze afnemer ook op «aan» heeft staat. Dit gegeven wordt eerst bevestigd (verstrekt) aan de afnemer. Na plaatsing van – meestal – een grote hoeveelheid berichten ontvangt de verzendende afnemer een bevestiging van bezorging in MijnOverheid, of het falen daarvan, onder vermelding van de betreffende BSN's.

Voor afnemers die de Berichtenbox wel als verplicht kanaal hebben aangewezen (vooralsnog alleen de Belastingdienst) heeft het gegeven «berichtenvoorkeur» zijn betekenis verloren. Die staat immers altijd op «aan». Wel wordt – net als bij de andere afnemers – het bestaan van de Berichtenboxen waarop moet worden afgeleverd en vervolgens de daadwerkelijke aflevering van berichten, dan wel het falen daarvan, bevestigd onder vermelding van de betreffende BSN's.

Om die afnemer wel in staat te stellen de invoering van het gebruik van MijnOverheid als verplicht kanaal adequaat te kunnen monitoren en bijvoorbeeld de bijbehorende communicatiecampagne goed te kunnen uitvoeren, wordt op diens verzoek bevestigd (of ontkend) dat een gebruiker zijn account in gebruik heeft genomen/heeft gepersonaliseerd.

5.7. Informatiebeveiliging

Indien er zich een incident heeft voorgedaan waarbij de integriteit, vertrouwelijkheid of beschikbaarheid van het systeem in het geding is geweest, worden alle betrokken gegevens vastgelegd en geanalyseerd. Dit om de oorzaak te kunnen achterhalen en eventuele gevolgen te kunnen herstellen. Omdat dit soort onderzoeken zeer tijdrovend zijn en het belang groot, is het noodzakelijk om voor de betrokken gegevens waarvoor een initiële bewaartermijn geldt van 18 maanden of 1 jaar te verlengen tot 36 maanden. Deze termijn is gebaseerd op best practices.

6. Aspecten gegevensverwerking DigiD, DigiD Machtigen en MijnOverheid

6.1 Gebruikersondersteuning

Voor de ondersteuning van gebruikers van MijnOverheid, DigiD en DigiD Machtigen zijn klantcontactcentra («helpdesk») beschikbaar, die telefonisch of schriftelijk/per e-mail vragen en klachten in behandeling nemen en daarvan een registratie bijhouden.

Omdat de accounts in de drie voorzieningen primair gebaseerd zijn op BSN dient dit ook voor gebruikersondersteuning te worden verwerkt. Passend bij de vraag of klacht worden daarvoor de noodzakelijke persoonsgegevens verwerkt, meestal gelijk aan de account- of gebruiksgegevens. In voorkomend geval aangevuld met een telefoonnummer of een extra email-adres. De hoeveelheid keren contact en de tijd die gemoeid is met het beantwoorden van vragen en oplossen van problemen of klachten varieert. Soms is een vraag meteen beantwoord. Bij complexere of terugkerende problemen is er gedurende langere tijd meerdere keren contact met dezelfde gebruiker. Passend bij die praktijk is de bewaartermijn gesteld op 18 maanden, waarbij tevens rekening is gehouden met de lengte van het klachtrecht van hoofdstuk 9 van de Awb.

Aangezien persoonsgegevens, waaronder het BSN, worden verwerkt in de voorzieningen waarvoor hij een zorgplicht draagt, is de Minister van BZK verantwoordelijk voor privacybescherming. Voor wat betreft de

gebruikersondersteuning met betrekking tot die voorzieningen geldt, dat hierbij moet worden onderscheiden tussen eerstelijns ondersteuning (klantcontactcentra) en tweedelijns ondersteuning («backoffice»). De eerstelijns ondersteuning geschiedt door een hiertoe gecontracteerd private partij; hiermee is namens de Minister van BZK als verantwoordelijke een bewerkerovereenkomst gesloten. In de bewerkersovereenkomst zijn onder meer bepalingen opgenomen over de verplichtingen van de opdrachtnemer inzake het verwerken van persoonsgegevens en de beveiliging hiervan. De tweedelijns ondersteuning maakt deel uit van de beheerstaak met betrekking tot de voorzieningen. Hiervoor is de Minister van BZK verantwoordelijk en moet hij voldoen aan de bepalingen inzake de bescherming van persoonsgegevens in het onderhavige Besluit en aan de beveiligingsmaatregelen die gelden ingevolge de Regeling voorzieningen GDI.

6.2. Het borgen van de beveiliging en betrouwbaarheid van de voorziening

In de Wet EBV is in artikel X opgenomen dat de zorgplicht het borgen van de beveiliging en de betrouwbaarheid van de voorzieningen omvat. In de toelichting bij artikel X van de Wet EBV is al aangegeven dat daarmee wordt beoogd de verwerking van persoonsgegevens mogelijk te maken om misbruik of oneigenlijk gebruik van de bedoelde voorzieningen te voorkomen of te beëindigen. Op die manier kunnen burgers, maar ook de overheid zelf, in hun belangen worden beschermd als misbruik of oneigenlijk gebruik wordt gemaakt van de voorzieningen. Zo kan indien nodig, bijvoorbeeld wanneer een DigiD-activeringscode in verkeerde handen is gekomen, de desbetreffende DigiD worden ingetrokken of geblokkeerd om de betrouwbaarheid van de voorziening te waarborgen en (verdere) schade voor de burger of de overheid te voorkomen. Ook kan (de beschikbaarheid van) een voorziening als zodanig (tijdelijk) worden onderbroken om bijvoorbeeld een beveiligingsprobleem op te kunnen lossen. Over deze maatregelen zijn bepalingen opgenomen in de Regeling voorzieningen GDI op grond van artikel X, tweede lid, van de Wet EBV.

Bij oneigenlijk gebruik of misbruik kan het zowel gaan om (bewuste) aantastingen van en inbreuken op de technische beveiliging (hacken, DDoS-aanvallen) als om (bewuste) inbreuken op de processen van de voorzieningen («fraude»). De genoemde zorgplicht van de Minister van BZK omvat bijvoorbeeld het voorkomen of bestrijden van compromittering van DigiD. Dat houdt in zowel compromittering van het systeem als zodanig als van individuele DigiD's. Dat laatste betreft bijvoorbeeld de situatie waarin een DigiD activeringscode of inlogcode (gebruikersnaam en wachtwoord) wordt gebruikt door een ander dan degene aan wie het bij inloggen gebruikte BSN is toegekend, zonder dat de rechtmatige houder van dat DigiD dat weet.

Er zijn ook situaties waarin een DigiD op zichzelf niet is gecompromitteerd (het proces werkt dan conform verwachting), maar waarin anderszins sprake is van misbruik of oneigenlijk gebruik. Zo kan een DigiD activeringscode of inlogcode worden gebruikt door een ander dan degene aan wie het bij inloggen gebruikte BSN is toegekend met instemming van de rechtmatige houder.

Het kan ook nodig zijn om persoonsgegevens te verwerken om te controleren of burgers geen slachtoffer worden van reeds bekende en redelijkerwijs te onderkennen vormen van misbruik van de voorziening.

De Minister van BZK kan uit hoofde van de genoemde zorgplicht controles en onderzoek op de gegevens uitvoeren, waaruit signalen kunnen voortvloeien van misbruik of oneigenlijk gebruik. Logius kan zo ongebruikelijke stramienen her- of onderkennen (zogenoemd a-typisch

gebruik), die kunnen duiden op misbruik of oneigenlijk gebruik. Denk aan situaties waarin grote aantallen DigiD's vanuit een zelfde plaats op ongebruikelijke (nachtelijke) tijden worden aangevraagd en overeenkomsten vertonen in gebruik bij verschillende afnemers. Een ander signaal bijvoorbeeld is dat één mobiel telefoonnummer hoort bij meerdere DigiD- accounts. Deze signalen kunnen duiden op misbruik of oneigenlijk gebruik, maar dat hoeft niet: in het geval van het mobiele telefoonnummer kan het ook zo zijn dat iemand vergeten is zijn nieuwe nummer door te geven en zijn oude nummer inmiddels aan iemand anders is uitgegeven. Dergelijke signaleringen zullen derhalve altijd door menselijke tussenkomst worden beoordeeld alvorens verder te worden opgepakt, zodat het treffen van averechtse maatregelen wordt voorkomen.

Voor zover het noodzakelijk is om uit te zoeken of inderdaad sprake is van misbruik of oneigenlijk gebruik, kan de Minister van BZK persoonsgegevens verwerken en ook gegevens ontvangen van bijvoorbeeld afnemers die misbruik met bepaalde BSN's vermoeden of gegevens verstrekken aan afnemers die behulpzaam kunnen zijn in de constatering of inderdaad sprake is van misbruik of oneigenlijk gebruik.

De voorzieningen vormen onderling een samenspel in de digitale keten. Een burger logt met DigiD, al dan niet met gebruikmaking van DigiD Machtigen, in bij MijnOverheid om vervolgens zaken te kunnen regelen met afnemers. Dit samenspel in de keten zorgt ervoor dat misbruik en aantastingen zich ook in ketenverband (kunnen) afspelen. Voor een effectieve aanpak van misbruik en oneigenlijk gebruik is het daarom noodzakelijk om tussen de voorzieningen onderling gegevens met elkaar in verband te kunnen brengen en het misbruik «uit de keten» te kunnen halen.

In het onderzoek naar misbruik zou kunnen blijken dat er geen sprake is van misbruik of oneigenlijk gebruik van DigiD, een machtiging of een MijnOverheid-account, maar dat met op zich rechtmatig gebruik van DigiD een frauduleuze aanvraag voor bijvoorbeeld toeslagen wordt ingediend bij een bestuursorgaan (een individuele burger pleegt aldaar zelf misbruik). Aangezien er dan geen sprake is van aantasting van de betrouwbaarheid van de voorzieningen, kan de zorgplicht van artikel X geen grondslag meer vormen voor gegevensverwerking. Eventuele voortgezette verwerking van gegevens in het kader van bijvoorbeeld het meewerken aan het onderzoek van het bestuursorgaan dat met de fraude is geconfronteerd of aan strafrechtelijk onderzoek, kan alleen voor zover dat op grond van de Wbp of andere sectorale wetgeving mogelijk is.

Voor dit besluit is relevant welke gegevens in het kader van het controleren van gegevens in verband met voorkomen of beëindigen van misbruik en oneigenlijk gebruik worden verwerkt. Kenmerk van misbruik en oneigenlijk gebruik is dat van tevoren niet kan worden bepaald hoe dat plaatsvindt en welke gegevensverwerking nodig is om de betrouwbaarheid te borgen en de burger in zijn belang te beschermen. Om die redenen kan niet op voorhand een inperking worden aangebracht in de gegevens die dienen te worden verwerkt en verstrekt. De verwerking kan daarmee in potentie ieder gegeven betreffen dat beschikbaar is binnen de voorziening. Hieronder wordt onder het kopje «Bewaartermijn van 5 jaar voor gebruiksgegevens» verder ingegaan op de bewaartermijn van deze gegevens in relatie tot de controles in verband met misbruik/oneigenlijk gebruik.

In het geval van compromittering van DigiD, een machtiging of een MijnOverheid-account kan de rechtmatige houder ervan schade ondervinden als gevolg van het misbruik of oneigenlijk gebruik ervan door een

ander. Hij zal dan ook benaderd moeten worden, wat doorgaans per brief zal gebeuren. Daartoe kunnen dan de bij het betrokken BSN behorende naam- en adresgegevens uit de BRP worden verstrekt; zodra correspondentie met de betrokken gebruiker niet meer nodig is, zullen deze gegevens maximaal 6 weken worden bewaard. Hetzelfde geldt voor de gebruiker aan wie per brief wordt medegedeeld dat hij wordt uitgesloten van verder gebruik van DigiD, totdat hij opnieuw een DigiD heeft aangevraagd.

Voor de volledigheid wordt opgemerkt dat hetgeen in deze paragraaf is beschreven ten aanzien van het voorkomen en beëindigen van misbruik en oneigenlijk gebruik van DigiD analoog geldt ten aanzien van de andere voorzieningen waarop dit besluit ziet. De kans op en mogelijkheden voor misbruik en oneigenlijk gebruik zijn echter op dit moment, gezien de langere bestaanshistorie, nog voornamelijk geconcentreerd bij DigiD. Echter deze mogelijkheden zullen met de brede en grootschalige uitrol – waarbij het gebruik van DigiD Machtigen en MijnOverheid naar verwachting exponentieel zal stijgen en voor burgers in bepaalde gevallen de enige wijze van contact met de overheid zal worden –, hoezeer ook getracht wordt deze te voorkomen, als onvermijdelijk en ongewenst neveneffect meegroeien.

6.3. Bewaartermijn van 5 jaar voor bepaalde gegevens

De bewaartermijn die in dit besluit is vastgesteld voor bepaalde gegevens is 5 jaar. De motivering van deze bewaartermijn verdient afzonderlijk aandacht in deze nota van toelichting.

Tot het moment van totstandkoming van dit besluit was de bewaartermijn van onder andere de gebruiksgegevens die in het kader van DigiD werden verwerkt 18 maanden. DigiD Machtigen en MijnOverheid hadden zich bij die bewaartermijn aangesloten. Deze bewaartermijn was gebaseerd op de praktijk op dat moment. Gebruikers logden vaak nog (slechts) eenmaal per jaar in met hun DigiD ten behoeve van de belastingaangifte. Daardoor merkten gebruikers eventuele problemen pas na (ruim) een jaar op. Deze problemen werden dan in de daarop volgende maanden opgepakt, waarvoor het noodzakelijk was dat gegevens op dat moment nog beschikbaar waren. Verder speelde het klachtrecht van hoofdstuk 9 van de Awb een rol, waarin een bestuursorgaan niet verplicht is een klacht te behandelen indien die klacht betrekking heeft op een gedraging die langer dan een jaar voor indiening van de klacht heeft plaatsgevonden (art. 9:1, eerste lid, in samenhang met artikel 9:8, eerste lid, onder b, van de Awb). De termijn van 18 maanden was in het licht van het voorgaande een realistische termijn waarbinnen gebruikers geholpen konden worden als dat nodig was en hun gegevens niet onnodig lang werden bewaard.

Inmiddels is de praktijk veranderd. Met de verdere maatschappelijke integratie van de digitale overheid raken DigiD, DigiD Machtigen en MijnOverheid steeds meer vervlochten in de dagelijkse praktijk. Het aantal gebruikers neemt daarbij in intensiteit, diversiteit en in (financieel) belang steeds verder toe. De voorzieningen vormen steeds vaker een essentiële schakel in de keten waarbij afnemers en vaak ook burgers gehouden zijn gegevens over de onderlinge contacten in de regel voor langere tijd te bewaren. Bewaartermijnen van enige jaren zijn daarbij geen uitzondering. De onderhavige voorzieningen vormen bovendien steeds meer onderdeel van de processen zoals die zich tussen burgers en afnemers (overheden) voltrekken en het gebruik ervan zal direct van invloed kunnen zijn op de gelding van onderlinge rechten en verplichtingen.

De praktijk laat ook een tendens zien waarbij burgers zich vaker met vragen om hun gegevens tot de voorzieningen wenden. Het aantal vragen

van gebruikers over hun gebruiksgegevens die langer teruggaan dan 18 maanden is toegenomen. Vaak gaat het om vragen in verband met bewijsvoering in juridische geschillen of procedures. Veel burgers verwachten van de overheid dat zij de gevraagde informatie voor hen beschikbaar heeft.

Met de invoering van de Wet EBV en de daarin opgenomen verplichtstelling van de digitale weg voor contact met de Belastingdienst, zal het gebruik van in ieder geval MijnOverheid naar verwachting sterk toenemen, waarschijnlijk zelfs exponentieel. Dit geldt – gezien de ketenafhankelijkheid – ook voor aanverwante voorzieningen als DigiD en DigiD Machtigen. Het gebruik van de voorzieningen wordt voor veel burgers het enige punt waar zij nog op kunnen terugvallen en geholpen kunnen worden als zij problemen ondervinden. Zeker gezien de Belastingdienst, waarbij de mogelijkheid bestaat om tot in ieder geval 5 jaar jaren terug met afhandeling van bijvoorbeeld aangifte inkomstenbelasting of toeslagen bezig te zijn, kan het van belang zijn om gebruiksgegevens van de voorzieningen over die periode ter beschikking te hebben.

Daarnaast is het in de praktijk voorgekomen dat slachtoffers van misbruik of oneigenlijk gebruikt niet adequaat konden worden ondersteund, omdat het misbruik zich uitstrekte over een langere periode dan waarvan de gebruiksgegevens nog beschikbaar waren. Ook voor dit soort situaties draagt een langere bewaartermijn bij aan adequatere ondersteuning en bescherming van burgers in hun belang.

In de praktijk bij DigiD is, als onvermijdelijk neveneffect, met het breder gebruik van de voorzieningen ook de keerzijde – misbruik – toegenomen. Gezien de toename van het gebruik op dit moment, de verplichtstelling van het gebruik van de voorzieningen op grond van de Wet EBV voor contacten met de Belastingdienst en de financiële diensten die worden ontsloten, ligt het in reden om aan te nemen dat ook de aantrekkelijkheid voor diegene die er misbruik (proberen te) maken van de overige voorzieningen ook zal toenemen.

De geschetste praktijk en de verwachte ontwikkelingen in de vraag naar informatie over de verwerking van met name de gebruiksgegevens vraagt om een nieuwe afweging tussen het belang van de gebruiker om geholpen (en beschermd) te worden en het belang van de gebruiker dat zijn gegevens niet onnodig lang worden bewaard. Gelet op de zorgplicht van de Minister van BZK voor onder andere de beveiliging en betrouwbaarheid van de voorzieningen en gelet op het belang dat ook de burger en de afnemers (overheden) daarbij hebben (een betrouwbare voorziening kan bepaalde informatie leveren aan de gebruikers en afnemers ervan en een veilige voorzieningen voorkomt of bestrijdt misbruik ervan), is een nieuwe bewaartermijn van 5 jaar voor bepaalde gegevens in het licht van de geschetste praktijk en verwachte ontwikkelingen gerechtvaardigd.

7. De verwerking van gegevens in het kader van het BSN-Koppelregister

7.1 Doel en functie BSN-Koppelregister

Het BSN-Koppelregister is een nieuwe voorziening in het kader van de GDI, die een koppeling legt tussen een middel voor elektronische authenticatie en het BSN van de houder.

Doel van het BSN-Koppelregister is het gebruik van – vooralsnog alleen private – authenticatiemiddelen mogelijk te maken voor het afnemen van elektronische diensten in het publieke domein, namelijk bij overheidsor-

ganen en natuurlijke en rechtspersonen, niet zijnde overheidsorganen, die gerechtigd zijn het burgerservicenummer te gebruiken.

Het gaat dan bijvoorbeeld om het aanvragen van een vergunning of toeslag. Deze voorziening maakt het voor afnemers van MijnOverheid (bijvoorbeeld de Belastingdienst, het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Sociale Verzekeringsbank (SVB) en gemeenten) mogelijk om naast publieke authenticatiemiddelen (DigiD) ook private authenticatiemiddelen te accepteren.

Anders dan bij de andere GDI-voorzieningen heeft het BSN-Koppelregister geen directe relatie met gebruikers (houders van de authenticatiemiddelen); zij zullen niets merken van de voorziening als zodanig. Het is namelijk de private authenticatiedienst (bijvoorbeeld een telecombedrijf of bedrijf dat digitale producten levert) waarbij burgers een authenticatiemiddel aanvragen/aanschaffen. Die private authenticatiedienst schakelt het BSN-Koppelregister in wanneer de burger dit middel (tevens) wil gebruiken voor de afname van publieke diensten. Voor de houder heeft dit als voordeel dat hij, naast gebruik van een publiek authenticatiemiddel, ook met een privaat authenticatiemiddel in het publieke domein kan inloggen en publieke diensten kan afnemen. Door deze zogeheten «multimiddelen-benadering» wordt naar verwachting de (elektronische) dienstverlening door de overheid verbeterd en het gebruiksgemak voor burgers verhoogd.

Voor private authenticatiediensten geldt *geen verplichting* om authenticatiemiddelen voor het publieke domein te leveren. Zij mogen zich blijven toeleggen op het leveren van authenticatiemiddelen voor het private domein. Maar als ze het publieke domein willen bedienen, kan dit via het BSN-Koppelregister geschieden. Ook houders hoeven een privaat authenticatiemiddel niet in het publieke domein te gebruiken als zij dat niet willen. Publieke authenticatiemiddelen (DigiD, in de huidige en door te ontwikkelen versie) zijn en blijven bruikbaar in het publieke domein. Maar als houders hun private middel in het publieke domein willen gebruiken, en de desbetreffende publieke dienstverlener daar gelegenheid toe biedt, kan dit op de aangegeven wijze geschieden, dus via de deelnemende private authenticatiedienst en door tussenkomst van het BSN-Koppelregister. Dit vormt de kern van de introductie van het eID-stelsel. eID, en daarmee ook de werking van het BSN-Koppelregister, wordt in 2016 gedurende enkele maanden beproefd.

De ontwikkeling, dat private authenticatiemiddelen op een substantieel en hoog betrouwbaarheidsniveau, ook bruikbaar zijn binnen het publieke domein, maakt samen met de doorontwikkeling van publieke authenticatie (DigiD) en de wettelijke verankering van (andere) voorzieningen voor de GDI deel uit van de uitwerking van het Regeerakkoord, dat ten doel heeft digitaal communiceren door en met de overheid en betere publieke dienstverlening te bewerkstelligen.

7.2 Het koppelproces

Het BSN-Koppelregister functioneert slechts indien een publieke dienstverlener alsmede een leverancier van private authenticatiemiddelen hebben aangegeven het gebruik van een privaat authenticatiemiddel in het publieke domein mogelijk te willen maken. Om de koppeling tussen het authenticatiemiddel en het BSN van de gebruiker tot stand te kunnen brengen, is verificatie van de identiteit van de gebruiker nodig. Om deze verificatie te kunnen uitvoeren – artikel X van de Wet elektronisch berichtenverkeer Belastingdienst spreekt in dit verband van een goede vervulling van de taak, inhoudend de zorg voor veilige en betrouwbare

voorzieningen voor elektronische authenticatie – worden persoonsgegevens verwerkt. Het BSN-koppelregister verkrijgt deze persoonsgegevens van de private authenticatiedienst. Het proces werkt als volgt.

Een burger schaft een authenticatiemiddel aan bij een private authenticatiedienst.

Ten behoeve van deze aanschaf biedt hij de leverancier een geldig wettelijk identiteitsbewijs aan, waardoor een controle uitgevoerd kan worden op zijn identiteit. Op basis hiervan legt de leverancier ook zijn persoonsgegevens vast in zijn klantenadministratie. Het kan zijn dat de leverancier de gegevens van de desbetreffende persoon al eerder heeft vastgelegd en zijn identiteit al eerder heeft geverifieerd aan de hand van een geldig wettelijk identiteitsbewijs omdat deze persoon ook andere diensten bij hem afneemt, bijvoorbeeld voor internet of telefonie. De authenticatiedienst levert, indien de burger aangeeft het authenticatiemiddel ook in het publieke domein te willen gebruiken, vervolgens eenmalig een aantal van de bij het registratieproces verkregen persoonsgegevens aan bij het BSN-Koppelregister. Deze set bestaat uit op basis van toestemming door gebruiker verkregen naam, geboortedatum en het pseudo-ID van de gebruiker. De authenticatiedienst levert ook het BSN aan aan het BSN-Koppelregister. Dit kan echter niet op basis van toestemming door de gebruiker/burger, aangezien het BSN een bijzonder persoonsgegeven is in de zin van de Wet bescherming persoonsgegevens. Daarom geschiedt deze aanlevering op basis van een bewerkersovereenkomst tussen de Minister van BZK en de authenticatiedienst.

De Minister van BZK is – zoals eerder aangegeven – op grond van artikel X van de Wet elektronisch berichtenverkeer Belastingdienst verantwoordelijke voor de verwerking van het BSN door het BSN-Koppelregister en besteedt de aanlevering van het BSN ten behoeve van het koppelproces uit aan de authenticatiedienst. Anders gezegd: artikel X biedt voor de Minister van BZK een wettelijke basis, en biedt als afgeleide daarvan aan private partijen (authenticatiediensten) de basis om het BSN te verstrekken in de hoedanigheid van *bewerker* voor de Minister van BZK als verantwoordelijke en beheerder van het BSN-Koppelregister. In de bewerkersovereenkomst wordt onder meer opgenomen dat het BSN ingevolge artikel 24, eerste lid, van de Wbp slechts zal worden verwerkt voor doeleinden bij de wet bepaald, dat de bewerkersovereenkomst slechts ziet op de verwerking van het BSN in het kader van de doorgifte aan het BSN-Koppelregister en dat de authenticatiedienst in zijn hoedanigheid van bewerker na de (eenmalige) aanlevering het BSN niet bewaart.

Om de verkregen gegevens te controleren op juistheid, vraagt het BSN-Koppelregister gegevens op uit de BRP. Voor het BSN als basis voor de uit te voeren controle («koppeling»), is gekozen omdat alleen op basis hiervan de grootst mogelijke zekerheid wordt verkregen omtrent de identiteit van de gebruiker. Als alternatief is overwogen om het nummer van het document als bedoeld in artikel 1 van de Wet op de Identificatieplicht te hanteren. Op zichzelf zou een WID-documentnummer geschikt zijn als basis voor de controle. Echter, het BSN is een meer betrouwbare en persistente manier om uniciteit te verzekeren. Hiermee is aan de eisen van noodzaak, proportionaliteit en dataminimalisatie voldaan. De Privacy Impact Assessment inzake het Introductieplateau eID-stelsel van 31 juli 2015 concludeert in dit verband dat het gebruik van BSN zoveel mogelijk wordt beperkt en alleen wordt gebruikt voor de doeleinden waarvoor dit daadwerkelijk nodig is. Nadat bij de controle de gegevens juist zijn gebleken, wordt de koppeling tussen het authenticatiemiddel en het BSN in het BSN-Koppelregister geregistreerd. De betreffende authenticatiedienst krijgt hiervan een melding. Het BSN-koppelregister controleert, aan

de hand van een hiertoe aangelegde controlelijst, of de desbetreffende publieke dienstverlener het met succes gekoppelde BSN mag ontvangen. Indien deze stappen met goed gevolg zijn doorlopen, levert Het BSN-Koppelregister vervolgens bij iedere sessie waarbij de burger inlogt met zijn authenticatiemiddel aan de publieke dienstverlener het gekoppelde BSN op een beveiligde, privacybeschermende (= versleutelde) manier, waardoor alleen de publieke dienstverlener waarbij wordt ingelogd het BSN kan lezen. Op deze manier is het middel geschikt gemaakt voor gebruik in het publieke domein.

7.3. Persoonsgegevens

In het kader van het BSN-Koppelregister wordt door de Minister van BZK een limitatieve set van persoonsgegevens verwerkt, namelijk: naam (voornamen, voorvoegsel, geslachtsnaam e/o achternaam), geboortedatum, datum van overlijden, het BSN en het pseudo-ID op het authenticatiemiddel (artikel 5, onderdelen a tot en met c), met als doel de verificatie van de identiteit van de houder van een authenticatiemiddel, die dit middel wil gebruiken in het publieke domein. Om uniciteit van de houder te kunnen vaststellen, is de set gegevens («attributen») zo effectief en minimaal mogelijk gehouden.

De datum van registratie van de koppeling (artikel 5, onderdeel d) wordt vastgelegd om de afnemer te kunnen berichten dat deze houder gevalideerd is en dat hij in het vervolg publieke diensten met het desbetreffende middel mag afnemen. Het tijdstip van inloggen bij de publieke dienstverlener (artikel 5, onderdeel e) wordt vastgelegd om redenen van een goede dienstverlening richting afnemers. Logging van – reeds beschikbare – gegevens dient eveneens beheersdoelen («doet het BSN-Koppelregister wat het moet doen»). Er vindt controle van de keten plaats ter detectie van eventuele systeemfouten en om de consistentie van het functioneren van de voorziening te waarborgen. In dit verband worden tevens audittrails uitgevoerd, teneinde managementinformatie te genereren en verantwoording te kunnen afleggen.

De naam, geboortedatum en datum van overlijden van de houder van een authenticatiemiddel worden na de controle met gegevens uit de BRP niet langer bewaard (artikel 14, onderdeel a). Na de registratie van de koppeling, hebben deze gegevens hun functie verloren. Bewaren is dan niet nodig en zou disproportioneel zijn. Voor de overige gegevens geldt een bewaartermijn van maximaal 18 maanden (na registratie van de koppeling) (artikel 14, onderdelen b tot en met e). Reden hiervoor is dat het BSN-Koppelregister in beginsel functioneert voor de duur van een proefperiode. De werking van het BSN-Koppelregister wordt in 2016 gedurende enkele maanden beproefd, waarbij de start, afronding en duur van de pilots verschillen per deelnemende publieke dienstverlener. Het ligt niet in de rede vooruit te lopen op definitieve invoering van de mogelijkheid om private middelen in het publieke domein te gebruiken. De bewaartermijn voor de gegevens in het BSN-koppelregister is daarom afgestemd op de tijd die maximaal nodig is voor het beproeven en het evaluatie. Een langere bewaartermijn is in dat verband onnodig en disproportioneel. Wanneer wordt besloten tot definitieve invoering, zullen de bewaartermijnen opnieuw worden bezien, met in achtneming van de uitkomsten van de laatst uitgevoerde stelsel-risicoanalyse en PIA.

7.4 Verstrekkingen

Instanties die publieke diensten verlenen zijn gerechtigd om het BSN te gebruiken (artikel 10 Wet algemene bepalingen burgerservicenummer). Teneinde elektronische diensten te kunnen verschaffen (bijvoorbeeld het

verlenen van een vergunning), moet de dienstverlener zekerheid hebben over het feit, dat een houder gerechtigd is deze diensten bij hem af te nemen en hiertoe een gevalideerd middel heeft. Deze zekerheid wordt verkregen via controle door het BSN-Koppelregister en het bij iedere transactie/inlog ontvangen van een versleuteld BSN, gekoppeld aan het authenticatiemiddel (artikel 9).

8. Privacykader

8.1 Inleiding

Dit besluit bevat bepalingen die een aanvulling zijn op de Wet bescherming persoonsgegevens (Wbp). Op grond van artikel X van de Wet EBV wordt, zoals hiervoor in de inleiding ook al is vermeld, geregeld welke persoonsgegevens in verband met de zorgplicht van de Minister van BZK ten aanzien van de voorzieningen DigiD, DigiD Machtigen, MijnOverheid en het BSN-Koppelregister worden verwerkt, aan wie ze worden verstrekt en wat de bewaartermijnen zijn. Voor alles wat dit besluit niet regelt over de verwerking van persoonsgegevens in het kader van deze voorzieningen, bijvoorbeeld het recht op inzage en correctie, gelden de bepalingen van de Wbp.

In dit hoofdstuk van de nota van toelichting zal aandacht worden besteed aan de overwegingen die met betrekking tot de (belangrijkste) onderdelen van dit besluit hebben geleid tot het oordeel dat de voorgestelde bepalingen voldoen aan de nationale en internationale normen op het terrein van de bescherming van de persoonlijke levenssfeer.

Hierna zal in paragraaf 8.2 worden ingegaan op de verhouding van het besluit tot de algemene beginselen betreffende de bescherming van de persoonlijke levenssfeer, zoals deze zijn gewaarborgd in onder andere artikel 10 van de Grondwet, artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM),[4] het Dataprotectieverdag[5] en het bijbehorende Protocol[6], de op deze verdragen gebaseerde jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) en artikel 8 van het Handvest van de grondrechten van de Europese Unie.[7]

Daarna wordt in paragraaf 8.3 ingegaan op enkele aspecten van de Wbp die in het kader van de gegevensverwerking in de genoemde voorzieningen specifieke aandacht verdienen.

Ten slotte wordt in paragraaf 8.4 ingegaan op de uitgevoerde privacy impact assessments en een reactie daarop gegeven.

---

[4] Rome, 4 november 1950, Trb. 1951, 154 (Nederlandse vertaling in Trb. 1990, 156).

[5] Het op 28 januari 1981 te Straatsburg tot stand gekomen Verdrag van de Raad van Europa ter bescherming van personen met het oog op de geautomatiseerde verwerking van persoonsgegevens, Trb. 1988,7 (Nederlandse vertaling in Trb. 1988, 7).

[6] Het op 8 november 2001 te Straatsburg tot stand gekomen Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdende verkeer van gegevens, Trb. 2003, 122 (Nederlandse vertaling in Trb. 2003, 165 en Trb. 2004, 288).

[7] Handvest van de grondrechten van de Europese Unie van 7 december 2000, als aangepast op 12 december 2007 te Straatsburg (PbEU 2010, C 83). Zie verder artikel 6 van het Verdrag betreffende de Europese Unie.

8.2 Toetsing van het besluit aan de Grondwet, internationale verdragen en het Handvest van de grondrechten van de Europese Unie

Artikel 10, eerste lid, van de Grondwet

Ingevolge artikel 10, eerste lid, van de Grondwet heeft iedereen recht op eerbiediging van zijn persoonlijke levenssfeer. De verwerking van persoonsgegevens over een burger vormt een inbreuk op diens persoonlijke levenssfeer. Dit is bij de verwerking van persoonsgegevens in het kader van de genoemde voorzieningen temeer aan de orde, omdat deze verwerking, gelet op het verplichte elektronische berichtenverkeer met de Belastingdienst op grond van de Wet EBV, voor het overgrote deel van de burgers niet op basis van vrijwilligheid plaatsvindt. Het recht op eerbiediging van de persoonlijke levenssfeer kan blijkens artikel 10, eerste lid, van de Grondwet evenwel bij of krachtens de wet worden beperkt. Aan de eis dat de beperking bij of krachtens de wet dient plaats te vinden, wordt met dit besluit voldaan, gelet op de wettelijke grondslag voor de gegevensverwerking in artikel X van de Wet EBV. De rechtvaardiging voor de inbreuk die door de gegevensverwerking in het kader van de betrokken voorzieningen op de persoonlijke levenssfeer van de betrokkenen wordt gemaakt, komt hierna aan de orde.

Artikel 8 van het EVRM

Artikel 8 van het EVRM beschermt het recht op respect voor het privéleven. Dit recht is evenwel niet absoluut. Ingevolge artikel 8 van het EVRM is een inmenging in de uitoefening van dit recht gerechtvaardigd, wanneer deze bij de wet is voorzien, tegemoet komt aan een legitiem doel en in een democratische samenleving noodzakelijk is in verband met een of meer in het tweede lid genoemde belangen. De wet dient bovendien afdoende waarborgen te bevatten om willekeur en misbruik te vermijden. Volgens de jurisprudentie van het EHRM is een inmenging noodzakelijk in een democratische samenleving, wanneer er sprake is van een dringende maatschappelijke behoefte (*pressing social need*). Om de inbreuk op het recht op respect voor het privéleven gerechtvaardigd te doen zijn, dient blijkens de jurisprudentie voorts te zijn voldaan aan de voorwaarden van proportionaliteit (er dient een redelijke verhouding te bestaan tussen de ernst van de inbreuk en de zwaarte van het belang dat met de inbreuk wordt gediend) en subsidiariteit (er is geen alternatief, dat even effectief, maar minder ingrijpend is). Toetsing van dit besluit aan de hiervoor genoemde vereisten voor een gerechtvaardigde inbreuk op het in artikel 8 van het EVRM neergelegde recht van burger, zoals dit in de jurisprudentie van het EHRM nader is ontwikkeld, levert het volgende beeld op.

Wettelijke basis

Aan de eis dat de inmenging «bij de wet» is voorzien, wordt voldaan. Uit de jurisprudentie van het EHRM blijkt dat een beperking op verschillende wijze «bij de wet» kan zijn voorzien: dit kan een wet in materiële zin zijn, een beleidsregel of zelfs een in de jurisprudentie gevormde regel. Deze wet of regel moet echter wel voor de burger toegankelijk zijn en voorts zo precies zijn dat de burger in staat is zijn concrete gedrag daarnaar te richten.

De Regeling voorzieningen GDI heeft haar grondslag in artikel X van de Wet EBV, en wordt uitgewerkt in dit besluit op grond van het genoemde artikel X. Ook deze gegevensverwerkingen zijn volgens de bovengenoemde jurisprudentie «bij de wet» voorzien.

Kenbaarheid

Wat betreft de eis van toegankelijkheid van de wettelijke basis waarin de inbreuk is geregeld, geldt dat het besluit op behoorlijke wijze wordt bekendgemaakt. Hierbij kan worden opgemerkt dat het besluit een belangrijke bijdrage levert aan de transparantie van de gegevens die in het kader van de genoemde voorzieningen worden verwerkt. Deze gegevens zijn nu immers op een eenduidige wijze opgenomen in een besluit dat wordt gepubliceerd in het Staatsblad en on-line toegankelijk en vindbaar wordt gemaakt voor de daarin geïnteresseerde burgers, waar voorheen deze informatie voor DigiD, DigiD Machtigen en MijnOverheid op verschillende wijze werd aangeboden in de privacy-verklaringen en gebruiksvoorwaarden op de bijbehorende websites.

Voorzienbaarheid

Voorts dient de inbreuk op de persoonlijke levenssfeer voorzienbaar te zijn. Ook aan deze eis wordt voldaan. Het besluit bevat een heldere regeling met betrekking tot de persoonsgegevens die kunnen worden verwerkt, de instanties aan wie gegevens kunnen worden verstrekt en welke gegevens het daarbij betreft en de bewaartermijn van de gegevens De verantwoordelijke voor de gegevensverwerking en de doeleinden van de verwerking zijn helder opgenomen in artikel X van de Wet EBV zelf. De rechten en plichten van de burger en het toezicht op de gegevensverwerking door een onafhankelijke instantie zijn bijvoorbeeld onderwerpen die onder de Wbp vallen en die hierna wat betreft de rechten van de burger ook nog nader worden toegelicht.

Het feit dat de gegevensverwerking in het kader van de bedoelde voorzieningen primair bij algemene maatregel van bestuur wordt geregeld, doet op zich geen afbreuk aan de eis dat de inbreuk op de persoonlijke levenssfeer voorzienbaar moet zijn. Ook de verwerking van persoonsgegevens die is vastgelegd in een algemene maatregel van bestuur (of in een ministeriële regeling) moet aan dezelfde criteria van kenbaarheid, voorzienbaarheid, proportionaliteit en subsidiariteit voldoen als een in de wet zelf opgenomen regeling.

Op het punt van de voorzienbaarheid biedt artikel X van de Wet EBV bovendien een duidelijk richtinggevend kader voor de regeling bij algemene maatregel van bestuur. Zo bepaalt artikel X, derde lid, van de Wet EBV dat de Minister van BZK persoonsgegevens, waaronder het BSN, verwerkt voor zover dit noodzakelijk is voor de goede vervulling van de zorgtaak die hem in het eerste lid van artikel X van de Wet EBV is opgelegd, namelijk de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en elektronische registratie van machtigingen. In het derde lid is uitputtend vermeld dat bij algemene maatregel van bestuur nader wordt bepaald welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard.

Het feit dat in dit besluit, anders dan in de wet, de voorzieningen niet langer functioneel, maar concreet worden beschreven met de naam waaronder ze bij het publiek bekend zijn, draagt bij aan de voorzienbaarheid.

Legitiem doel

De inmenging die de gegevensverwerking maakt op het recht in artikel 8 van het EVRM, dient noodzakelijk te zijn in een democratische samenleving in verband met een aantal nader genoemde belangen. In artikel 8, tweede lid, van het EVRM wordt in dat verband gesproken over het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden en de bescherming van de rechten en vrijheden van anderen. Deze opsomming omvat in feite voor het grootste deel de taken die een moderne overheid voor zijn burgers vervult.

Met de Wet EBV wordt verplicht gebruik van de Berichtenbox ingevoerd voor berichten van de Belastingdienst. Bij invoering van verplicht gebruik van de Berichtenbox dient de verwerking van persoonsgegevens, gelet op artikel 8, onder e, van de Wbp, gebaseerd te zijn op een publiekrechtelijke taak. Deze taak is opgenomen in het eerste lid van artikel X van de Wet EBV. Om verplicht gebruik mogelijk te maken en het fiscale deel van het wetsvoorstel uitvoerbaar te laten zijn, behelst artikel X een algemene wettelijke basis voor de voorzieningen inzake de GDI in relatie tot burgers. Dit besluit, dat is gebaseerd op het derde lid, stelt regels met betrekking tot de verwerking van persoonsgegevens in verband met die taak.

Er is dan ook sprake van een dringende maatschappelijke behoefte (*pressing social need*) die de inmenging rechtvaardigt die de gegevensverwerking in de bedoelde voorzieningen maakt op het in artikel 8 van het EVRM genoemde recht van de burger.

Proportionaliteit

Wat betreft de eis van proportionaliteit bevat het besluit de nodige bepalingen die waarborgen dat er geen verdergaande inmenging plaatsvindt met het recht van betrokkene als bedoeld in artikel 8 van het EVRM dan noodzakelijk is. Het besluit is het resultaat van een zorgvuldige afweging tussen het belang van de overheid bij een doelmatige invulling van de zorgplicht die bij haar is neergelegd in artikel X, eerste lid, van de Wet EBV enerzijds en de bescherming van de persoonlijke levenssfeer van de gebruikers anderzijds. Dit uit zich in de eerste plaats in het feit dat de verwerking van persoonsgegevens beperkt is tot zo min mogelijk gegevens en alleen tot die gegevens van de burger die echt essentieel zijn om de voorzieningen beschikbaar te kunnen stellen, in stand te kunnen houden, te laten werken en beveiligen en betrouwbaar te houden. Het BSN speelt hierbij een cruciale rol. In de bedoelde voorzieningen wordt zoveel mogelijk enkel met het BSN gewerkt. Voor zover afnemers van de voorzieningen meer persoonsgegevens van de betreffende burger nodig hebben, zullen zij die via andere wegen moeten verkrijgen. Doorgaans zullen afnemers de voor hen noodzakelijk gegevens die behoren bij een bepaald BSN (dat zij in het kader van het gebruik van een burger van DigiD, DigiD Machtigen, MijnOverheid of een via het BSN-Koppelregister gevalideerd authenticatiemiddel verstrekt krijgen), verstrekt kunnen krijgen uit de BRP, mits uiteraard zij op grond van de Wet basisregistratie personen in aanmerking komen voor verstrekking van bepaalde gegevens uit de BRP. Op die manier is het aantal persoonsgegevens dat in het kader van de bedoelde voorzieningen wordt verwerkt, grotendeels beperkt tot het BSN en bijbehorende gebruiks- en accountgegevens. Met name voor het uitgifte- en identificatieproces worden (tijdelijk) ook naam, adres, geboortedatum en soms de nummers van het Nederlandse paspoort of een Nederlandse identiteitskaart gebruikt.

In het kader van de voorzieningen worden geen gevoelige persoonsgegevens verwerkt, zoals bijvoorbeeld gegevens over ras, politieke opvatting of geloof.

De proportionaliteit van de gegevensverwerking valt ook af te leiden uit de bepalingen over de bewaartermijnen van de gegevens, waarbij de bewaartermijn duidelijk is onderbouwd en beperkt tot het doel van de verwerking. Ook is duidelijk vastgelegd aan wie welke gegevens mogen worden verstrekt. De desbetreffende bepalingen waarborgen dat gegevens niet langer worden bewaard en niet meer gegevens worden verstrekt dan noodzakelijk.

Subsidiariteit

Ten slotte is er nog de vraag, of het doel dat met de voorzieningen wordt beoogd, ook op een andere, even effectieve, maar minder ingrijpende wijze zou kunnen worden bereikt. Van belang is dat dit besluit de bestaande praktijk bij de bedoelde voorzieningen vastlegt; in die zin is er bij de totstandkoming van dit besluit niet bekeken of een andere wijze dan gebruik van de bestaande voorzieningen mogelijk minder ingrijpend zou zijn. Aan het beleggen van de zorgplicht voor deze taken bij de Minister van BZK en de mogelijke risico's die dat met zich meebrengt voor de privacy, wordt hierna aandacht besteed in paragraaf 8.4 over de gehouden Privacy Impact Assessement inzake MijnOverheid, DigiD en DigiD Machtigen.

Dataprotectieverdrag

In het Dataprotectieverdrag zijn als belangrijkste principes voor een gerechtvaardigde gegevensverwerking opgenomen dat de gegevens rechtmatig moeten zijn verkregen, alleen voor specifieke en legitieme doeleinden mogen worden opgeslagen, evenredig moeten zijn in relatie tot het doel waarvoor ze zijn opgeslagen en niet langer mogen worden bewaard dan vereist is voor het doel waarvoor ze zijn opgeslagen. In het Aanvullende Protocol op het Dataprotectieverdrag is onder meer bepaald dat iedere bij het verdrag aangesloten staat een of meer autoriteiten verantwoordelijk stelt voor het toezicht op de naleving van de maatregelen in haar nationale recht waarmee uitvoering wordt gegeven aan de grondbeginselen vervat in de hoofdstukken II en III van het Verdrag en in het Protocol.

Aangezien het Dataprotectieverdrag uitwerking geeft aan artikel 8 van het EVRM is voor de uitleg van (bepaalde begrippen in) dit verdrag de uitleg die gegeven wordt aan artikel 8 van het EVRM van belang. Op de uitleg van artikel 8 van het EVRM is hiervoor uitvoerig ingegaan. Een aparte bespreking van de bepalingen in het Dataprotectieverdrag en het Aanvullend Protocol voegt aan hetgeen hiervoor is opgemerkt weinig toe. Gezien het voorgaande kan een aparte toets van het besluit aan verdrag en protocol achterwege blijven.

Artikel 8 van het Handvest van de grondrechten van de Europese Unie

Met de inwerkingtreding van het Verdrag van Lissabon per 1 december 2009 heeft het Handvest van de grondrechten van de Europese Unie dezelfde rechtskracht gekregen als de Europese verdragen. Het is overeenkomstig artikel 51 van het Handvest van toepassing op de handelingen van de Lidstaten voor zover zij uitvoering geven aan Unierecht, zoals in dit geval de Dataprotectierichtlijn. In artikel 8, eerste lid, van het Handvest wordt het recht op bescherming van persoonsgegevens gegarandeerd. Het tweede lid van die bepaling regelt dat de

gegevens eerlijk en voor bepaalde doeleinden worden verwerkt op basis van een gerechtvaardigde grondslag waarin de wet voorziet. Daarnaast moeten de rechten op inzage en rectificatie worden gegarandeerd. Het derde lid van die bepaling regelt dat een onafhankelijke autoriteit op de naleving van deze regels moet toezien. Het besluit voldoet, in samenhang met de van toepassing zijnde bepalingen van de Wbp inzake inzage en correctie en toezicht, aan de eisen die gesteld zijn in artikel 8, tweede en derde lid, van het Handvest (zie ook hieronder, onderdeel 8.3). Artikel 52, eerste lid, van het Handvest voorziet in de mogelijkheid van rechtvaardiging van een inmenging in de Handvestrechten. Ook aan de hieruit voortvloeiende vereisten is voldaan. De zorgplicht van de Minister van BZK voor de voorzieningen is wettelijk geregeld in artikel X van de Wet EBV. Daarnaast is de inperking te rechtvaardigen uit het oogpunt van een door de Unie geaccepteerd doel van algemeen belang. Hetgeen hierboven is gesteld bij de behandeling van artikel 8 van het EVRM ter rechtvaardiging van de proportionaliteit en subsidiariteit van de inmenging in het grondrecht op bescherming van de persoonlijke levenssfeer kan eveneens dienen ter rechtvaardiging van de beperking van het Handvestrecht op bescherming van persoonsgegevens.

8.3 De Wet bescherming persoonsgegevens

In deze paragraaf wordt aandacht besteed aan enkele aspecten van de Wbp die in het kader van de gegevensverwerking in de genoemde voorzieningen specifieke aandacht verdienen, namelijk de transparantie en de rechten van de burger.

Transparantie

In hoofdstuk 5 van de Wet bescherming persoonsgegevens zijn de zogenaamde transparantievoorschriften opgenomen. Daarbij wordt een onderscheid gemaakt tussen het geval dat de verkrijging van de gegevens bij de betrokkene zelf plaatsvindt (artikel 33) en dat waarbij de gegevens niet bij de betrokkene zijn verkregen (artikel 34). Ingevolge dit besluit vindt het verkrijging van de gegevens van de gebruikers van DigiD, DigiD Machtigen en MijnOverheid op beide wijzen plaats. Bij DigiD en DigiD Machtigen gaat het bijvoorbeeld om de gegevens die de burger zelf moet verstrekken op het moment dat hij een DigiD of registratie van een machtiging in DigiD Machtigen aanvraagt. Informatie die in het kader van DigiD, DigiD Machtigen en MijnOverheid buiten de betrokkene om wordt verkregen, zijn bijvoorbeeld gegevens die nodig zijn om ambtshalve MijnOverheid-accounts aan te maken, of gegevens over het gebruik van de voorzieningen door betrokkene.

In die gevallen waarin gegevens van de betrokkene zelf worden verkregen, moet de verantwoordelijke voor de verwerking van persoonsgegevens de betrokkene ten minste zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mededelen vóór het moment van verkrijging van de informatie van de betrokkene, tenzij de betrokkene daarvan reeds op de hoogte is (artikel 33 Wbp). Gezien de wijze waarop wettelijke voorschriften worden bekendgemaakt kan betrokkene in beginsel weliswaar geacht worden op de hoogte te zijn van de verwerking van hem betreffende gegevens in het kader van DigiD, DigiD Machtigen en MijnOverheid, maar dit ontslaat de uitvoerende instanties niet van de plicht al het mogelijke te doen om de betrokkene daarover in een zo vroeg mogelijk stadium actief te informeren.

In die gevallen waarin de gegevens niet van de betrokkene worden verkregen en de vastlegging en verstrekking van persoonsgegevens wettelijk is voorgeschreven, moet de verantwoordelijke de betrokkene op diens verzoek informeren over het wettelijk voorschrift dat tot de

vastlegging of verstrekking van de hem betreffende gegevens heeft geleid (artikel 34, vijfde lid, Wbp).

De Minister van BZK geeft in het kader van Digid, DigiD Machtigen en MijnOverheid uitvoering aan de transparantieverplichtingen door een privacyverklaring op de betreffende informatiewebsites waarin onder andere wordt aangegeven wie de verantwoordelijke is voor de verwerking van persoonsgegevens en met welk doel de persoonsgegevens worden verwerkt. Ook zal op de websites van de betreffende voorzieningen een link worden opgenomen naar de bijbehorende wet- en regelgeving, waaronder dit besluit en de bijbehorende nota van toelichting.

Rechten van de burger

In hoofdstuk 6 van de Wbp zijn de rechten van de burger vastgelegd over wie persoonsgegevens worden verwerkt. Het betreft, voor zover relevant in het kader van DigiD, DigiD Machtigen en MijnOverheid, het recht van inzage (artikel 35 Wbp) en het recht van correctie (artt. 36 tot en met 38 Wbp).

Het recht van inzage en correctie

Op grond van artikel 35 van de Wbp heeft de betrokkene het recht om te weten welke persoonsgegevens door de verantwoordelijke worden verwerkt, voor welke doeleinden en aan welke personen of instanties deze gegevens zijn verstrekt.

Op grond van de artikelen 36 tot en met 38 van de Wbp heeft de betrokkene het recht de verantwoordelijke te verzoeken hem betreffende gegevens te verbeteren, aan te vullen, af te schermen, of te verwijderen bij feitelijke onjuistheden, bij verwerking ten behoeve van onvolledige of niet ter zake dienende doelen of bij verwerkingen die in strijd met een wettelijk voorschrift worden verricht.

De wijze waarop Logius, namens de Minister van BZK, uitvoering geeft aan deze rechten van de burger, is vastgelegd in de privacyverklaringen van DigiD, DigiD Machtigen en MijnOverheid, die op de betreffende websites zijn te vinden.

Met betrekking tot de nieuwe voorziening BSN-Koppelregister is vanzelfsprekend het inzage- en correctierecht eveneens van toepassing.

Voor DigiD kan voor inzage en correctie ook een verzoek worden gedaan. Een deel van de persoonsgegevens is echter, na inloggen, ook op de website in te zien, zoals de gebruiksgeschiedenis tot 18 maanden terug, het BSN en e-mailadres.

Correctie van gegevens is bij DigiD alleen mogelijk voor de gegevens die voor het gebruik van DigiD nodig zijn, zoals de gebruikersnaam, het wachtwoord, het e-mailadres en het mobiele telefoonnummer; deze kan de gebruiker zelf wijzigen op de website.

Gegevens over het adres en de geboortedatum en het BSN zijn als zodanig niet te corrigeren: het adres wordt alleen gebruikt om eenmalig een brief met activeringscode of brief met betrekking tot vermoedens van misbruik te versturen en dat adres wordt op die momenten verkregen uit de BRP. Hetzelfde geldt voor de geboortedatum die in de BRP wordt gecontroleerd.

Voor DigiD Machtigen kan op de website een overzicht van de geregistreerde machtigingen en aanvragen worden ingezien. Behalve het overzicht kunnen ook details worden ingezien zoals de omschrijving en toelichting op de dienst, de aanvrager in geval van een machtiging en het historisch gebruik. Tevens biedt de website de mogelijkheid om machti-

gingen en aanvragen in te trekken of de looptijd van een machtiging aan te passen of nieuwe aanvragen te doen.

Ook via de Helpdesk (primair voor niet-digitaalvaardigen) kan deze informatie worden verkregen. De vertegenwoordigde wordt ook steeds op de hoogte gebracht van de aanvragen en activeringen van zijn machtigingen. Via de Helpdesk van DigiD Machtigen kan een gebruiker navragen of een specifieke machtiging of aanvraag is geregistreerd. Als de Helpdesk het nodig acht kan een overzicht van machtigingen en aanvragen per post worden toegezonden. Dit overzicht bevat geen details of historisch gebruik.

Voor MijnOverheid geschiedt inzage en correctie op verzoek. Een deel van de persoonsgegevens is echter, na inloggen, ook op de website in te zien, zoals de gebruiksgeschiedenis tot een aantal maanden (thans: 20 maanden) terug, het BSN en het e-mailadres. Verder is het recht op inzage en correctie beperkt tot de gegevens die in dit besluit zijn opgenomen en worden verwerkt in het kader van de zorgplicht van de Minister van BZK voor deze voorziening; voor de verwerking van persoonsgegevens die worden getoond in de functionaliteiten Berichtenbox, Lopende Zaken of Persoonlijke gegevens zijn de bestuursorganen verantwoordelijk die van die diensten van MijnOverheid gebruik maken; voor inzage of correctie van gegevens die in die functionaliteiten worden getoond, moet de betrokkene zich dus wenden tot het voor die gegevens verantwoordelijke dienstverlener.

8.4. Privacy impact assessment (PIA)

In verband met de overgang naar de publiekrechtelijke inbedding en de aanloop naar nieuwe eID-middelen en de verdere ontwikkeling van de diensten en functionaliteiten, is een privacy impact assessment (PIA) uitgevoerd door Net2Legal Consultants (in samenwerking met PBLQ HEC) met betrekking tot de voorzieningen MijnOverheid, DigiD en DigiD Machtigen (d.d. 11 september 2015). In verband met de introductie van het eID-stelsel en het BSN-Koppelregister is een PIA uitgevoerd door Mazars (d.d. 31 juli 2015).

MijnOverheid, DigiD en DigiD Machtigen

In de PIA met betrekking tot de voorzieningen MijnOverheid, DigiD en DigiD Machtigen staat de rol van de Minister van BZK als zorgplichtige voor de voorzieningen MijnOverheid, DigiD en DigiD-machtigen centraal. In dat verband levert de PIA input voor het onderhavige besluit. Aangezien op termijn de nog in voorbereiding zijnde Wet GDI de basis voor het onderhavige besluit zal vormen, dient de PIA mede ter voorbereiding van deze nieuwe wetgeving.

De conclusie van de PIA is dat er in de praktijk zeker aandacht is voor privacy bij de ontwikkeling en werking van de voorzieningen. De PIA signaleert daarbij wel enkele aandachtspunten. Ten eerste wordt aangegeven dat de aandacht voor privacy bij de ontwikkeling en de praktijk vooral een «praktijkonderwerp» is en (op onderdelen) niet formeel vastgelegd. Het onderhavige besluit, in samenhang met artikel X van de Wet EBV en de op dat artikel gebaseerde Regeling voorzieningen GDI, is daarop het antwoord. Daarin immers wordt een groot deel van die ontstane praktijk nu formeel vastgelegd. Met de in voorbereiding zijnde Wet GDI zal het formele kader verder worden gecomplementeerd. Dat betekent ook dat aandachtspunten en aanbevelingen uit de PIA die, gelet op de reikwijdte van artikel X van de Wet EBV, in het onderhavige besluit of de Regeling voorzieningen GDI niet kunnen worden verwerkt omdat deze aandachtspunten de werkingssfeer van de genoemde regelgeving

overstijgen, zullen worden opgepakt bij de voorbereiding van de Wet GDI. Ten tweede wordt er aandacht voor gevraagd dat bij het gebruik en (hergebruik) van gegevens, dit niet altijd strikt gekoppeld wordt aan de concrete doeleinden waarvoor gegevens door de Minister van BZK als zorgplichtige voor de voorzieningen verwerkt worden. In reactie daarop kan worden gemeld dat het doel van de gegevensverwerking die in het onderhavige besluit wordt geregeld, is vastgelegd in artikel X van de Wet EBV, namelijk de «inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid» van de voorzieningen. In hoofdstuk 2 van het algemeen deel van deze nota van toelichting is aangegeven, dat deze doelen meerdere processen bestrijken die ten aanzien van de genoemde voorzieningen te onderscheiden zijn, zoals het proces van aanvraag en/of activering van de diensten van de voorzieningen, Uitgebreid is toegelicht hoe en met welke meer concrete doelen (bijvoorbeeld identificatie of het versturen van activeringscodes) diverse gegevens worden verwerkt, waarbij voor bepaalde gegevens geldt dat deze voor diverse meer concrete doelen worden gebruikt. Uit de doelen vloeit vervolgens, geheel in lijn met de Wbp, de motivering voort van de in het besluit vastgelegde maximale bewaartermijnen.

Derde aandachtspunt is dat de verdeling van verantwoordelijkheden en zorgplichten tussen enerzijds de Minister van BZK als zorgplichtige voor de voorzieningen en anderzijds de afnemers (overheidsorganisaties) niet altijd even duidelijk is. Met name voor de burger zou een concreet overzicht van «wie waar verantwoordelijk voor is» een bijdrage kunnen leveren. Wat het onderhavige besluit betreft is de verantwoordelijkheid van de Minister van BZK wat betreft de reikwijdte van het besluit (welke persoonsgegevens worden verwerkt, aan wie worden deze verstrekt en hoe lang worden deze bewaard) voldoende vastgelegd. Het onderhavige besluit gaat niet over de verantwoordelijkheden van de afnemers. In de toelichting bij de Regeling voorzieningen GDI op grond van artikel X van de Wet EBV wordt aan de verantwoordelijkheid van de afnemers wel aandacht besteed; overigens zal dat een aandachtspunt blijven bij de in voorbereiding zijnde Wet GDI.

Het vierde aandachtspunt is dat een eventuele langere bewaartermijn van 5 jaar voor bepaalde gegevens nog onvoldoende is afgewogen. Die afweging is inmiddels afgerond en heeft voor bepaalde gegevens geleid tot een gemotiveerde en afgewogen verlening van 18 maanden naar 5 jaar; zie hiervoor paragraaf 6.3 van het algemeen deel van deze nota van toelichting.

Resteren twee belangrijke aandachtspunten en aanbevelingen. De eerste aanbeveling is om maatregelen te treffen om de gegevensverwerking in het kader van de generieke voorzieningen (uitgifte en gebruik) wettelijk te voorzien van een adequate en strikte afscherming met een strikte doelbinding en een strikte geheimhoudingsverplichting en zorg te dragen voor een adequate organisatorische onafhankelijkheid van de beheerder (zorgplichtige) van de generieke voorzieningen ten opzichte van de Minister van BZK en ten opzichte van de afnemende overheidsorganisaties. De achtergrond van deze aanbevelingen is dat vanuit privacy bezien (zowel het grondrecht op bescherming van de persoonlijke levenssfeer als de verwerking van persoonsgegevens) kenmerkend is dat de Minister van BZK een bijzondere positie inneemt met specifieke privacyrisico's. Het risico voor de privacy is dat de Minister van BZK *de facto* de mogelijkheid heeft om het gedrag van burgers (hun relaties en contacten met de overheid) in kaart te kunnen brengen en te kunnen volgen. Wat de privacy en met name het grondrecht op bescherming van de persoonlijke levenssfeer en de risico's betreffende mogelijk hergebruik van gegevens over vooral het gebruik van de voorzieningen door de burger (o.a. de logfiles) betreft, komt de PIA tot de conclusie dat de huidige opzet (met generieke voorzieningen, toebedeling van alle taken en

werkzaamheden voor de voorzieningen aan de Minister van BZK en zonder specifieke wettelijke afscherming met onder andere geheimhoudingsbepalingen voor de gegevens betreffende de voorzieningen) tezamen bezien wordt ontraden wegens strijd, dan wel onnodige spanning met artikel 8 EVRM en ook het noodzakelijkheidsbeginsel van de Wbp, tenzij de genoemde aanbevolen maatregelen worden genomen.

Wat betreft de geheimhouding is in reactie op de PIA in het besluit opgenomen dat de Minister van BZK, los van de meer reguliere verstrekking van gegevens in verband met de diensten die de voorzieningen leveren, geen persoonsgegevens aan derden verstrekt zonder toestemming van de gebruiker of bezoeker (artikel 10). De enige uitzondering daarop is gegevensverstrekking aan overheidsorganen of rechtspersonen met een wettelijke taak die noodzakelijk is voor de borging van de beveiliging en betrouwbaarheid van de betreffende voorziening of verstrekking waartoe de Minister van BZK op grond van andere wettelijke bepalingen gerechtigd is.

Voor maatregelen in dit besluit met betrekking tot een adequate organisatorische onafhankelijkheid van de beheerder (zorgplichtige) van de generieke voorzieningen ten opzichte van de Minister van BZK en ten opzichte van de afnemende overheidsorganisaties biedt artikel X van de Wet EBV geen grondslag. Dit punt zal dan ook worden opgepakt in het kader van de voorbereiding van de Wet GDI.

De tweede belangrijke aanbeveling is dat gebruik van gegevens in het kader van misbruik en oneigenlijk gebruik, zeker daar waar het de belangen van de afnemers dient, gebaseerd dient te zijn op een specifieke wettelijke basis. Deze aanbeveling vloeit voor uit de constatering in de PIA dat het huidige gebruik van gegevens in het kader van misbruik en oneigenlijk gebruik niet enkel doelen dient die direct samenhangen met de rol van de Minister van BZK als zorgplichtige voor de voorzieningen, maar ook belangen van (enkel) de afnemende overheidsorganisaties. Het zojuist genoemde artikel 10 kan dienen als de wettelijke basis voor gegevensverstrekking in verband met misbruik en oneigenlijk gebruik voor die gevallen waarin de verstrekking samenhangt met de rol van de Minister van BZK. In hoofdstuk 6 van deze nota van toelichting is ingegaan op het feit dat de zorgplicht van artikel X van de Wet EBV geen grondslag biedt voor gegevensverwerking (en daarmee ook niet voor verstrekking) indien in onderzoek naar misbruik en oneigenlijk gebruik zou blijken dat er geen sprake is van misbruik of oneigenlijk gebruik van DigiD, een machtiging of een MijnOverheid-account, maar dat met op zich rechtmatig gebruik van DigiD een frauduleuze aanvraag voor bijvoorbeeld toeslagen wordt ingediend bij een bestuursorgaan. In die gevallen kan eventuele voortgezette verwerking (en verstrekking) van gegevens alleen voor zover dat op grond van de Wbp of andere sectorale wetgeving mogelijk is. Bij de voorbereiding van de Wet GDI zal meegenomen worden of aanvullende bepalingen in de Wet GDI zelf nodig of wenselijk zijn.

BSN-Koppelregister

In verband met de introductie van het eID-stelsel is een afzonderlijke PIA uitgevoerd. Vanwege de cruciale betekenis in het stelsel van het BSN-Koppelregister, bevat de PIA terzake enkele aandachtspunten. Geconcludeerd wordt primair, dat in het stelsel uitdrukkelijk aandacht is besteed aan technische en procedurele maatregelen waarmee de privacybescherming van burgers en consumenten zijn bevorderd en dat het maximale is gedaan om de privacy van houders te beschermen. De PIA onderkent tegelijkertijd een aantal resterende risico’s aangaande de privacybescherming binnen het Introductieplateau eID-stelsel en beveelt aan om op deze risico’s een aantal aanvullende procedurele maatregelen te treffen. Het gaat daarbij, voor wat betreft wet- en regelgeving, om

verankering van het gebruik van BSN binnen het private domein. Hierin wordt voorzien middels het samenstel van artikel X van de wet EBV, het onderhavige besluit en de Regeling voorzieningen GDI.

Voorts beveelt de PIA aan de bewaartermijnen zover mogelijk te minimaliseren (in ieder geval korter dan 7 jaar), zeker voor meer gevoelige persoonsgegevens, en bij voorkeur te differentiëren. Hieraan is voldaan met dit besluit, aangezien de maximale bewaartermijn voor de gegevens in het BSN-Koppelregister op 18 maanden is gesteld. Tenslotte bevat de PIA enkele aanbevelingen voor het geval het eID-stelsel een definitief karakter krijgt. Hierop wordt in dit besluit niet vooruit gelopen. Bij de voorbereiding van de wet GDI zal worden bezien of het opportuun is deze aanbevelingen mee te nemen.

9. Uitvoeringslasten, financiële gevolgen en regeldruk

9.1. Uitvoeringslasten en financiële gevolgen

Met dit besluit wordt de praktijk van gegevensverwerking, bewaring en verstrekking in drie bestaande ICT-voorzieningen gecodificeerd. Tevens wordt de voorgenomen gegevensverwerking door het BSN-Koppelregister beschreven. Deze vier voorzieningen vallen allen onder de verantwoordelijkheid van de Minister van BZK en worden uitgevoerd door Logius, de dienst digitale overheid, tevens dienstonderdeel van het Ministerie van BZK. De (jaarlijkse) kosten die gemoeid zijn met uitvoering en instandhouding van deze voorzieningen worden gedekt door de financiële afspraken die in samenspraak met de aangesloten afnemers en de Digicommissaris te dien aanzien zijn gemaakt of zijn bepaald in het betreffende programma. Dit betekent dat de uitvoeringslasten die voortvloeien uit dit besluit enkel een marginale kostenverhoging op het geheel bezien kan betekenen, bijvoorbeeld om de verlengde bewaartermijn in dit voorstel te kunnen uitvoeren.

9.2. Regeldruk

Het voorstel heeft enkel gevolgen voor de overheid. De overheid behoort echter niet tot de doelgroepen van de regeldrukoperatie van het kabinet.

In dit voorstel wordt enkel geregeld wat er met persoonsgegevens gebeurt. Er zijn dus enkel gevolgen voor overheden. Burgers of bedrijven hoeven geen extra handelingen te verrichten.

10. Consultatie

Een ontwerp van dit besluit is voor advies voorgelegd aan het College bescherming persoonsgegevens (CBP, per 1 januari 2016 Autoriteit Persoonsgegevens). Verder is het ontwerp van 22 september 2015 tot 19 oktober 2015 in consultatie geweest op internet. In de internetconsultatie werden 6 reacties ontvangen (waarvan 3 openbaar).

10.1 Advies van het College bescherming persoonsgegevens

Het CBP bracht op 3 december 2015 zijn advies uit (z2015-00766). In het onderstaande wordt hierop ingegaan.

De Berichtenbox als openbaar elektronische communicatiedienst

Het CBP merkt vooraf op dat de Berichtenbox van MijnOverheid mogelijk beschouwd moet worden als een openbare elektronische communicatiedienst als bedoeld in artikel 1.1, onderdeel f, van de

Telecommunicatiewet. Het CBP adviseert om, mocht de Berichtenbox inderdaad als zodanig kwalificeren, aan de mogelijke gevolgen hiervan aandacht te besteden in hoofdstuk 8 van de nota van toelichting.

De vraag van het CBP moet ontkennend worden beantwoord, gelet op artikel 1.1, onderdeel f juncto g en h van de Telecommunicatiewet. Als (openbare) elektronische communicatiedienst wordt aangemerkt een dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken, waaronder telecommunicatie-diensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch *niet* de dienst waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Bij de Berichtenbox gaat het om een dienst die met behulp van een internettoegangsdienst overgebrachte inhoud levert, en niet hoofdzakelijk bestaat uit het overbrengen van signalen. Hetzelfde is bijvoorbeeld het geval bij webmail, een dienst waarbij vanaf elke computer toegang tot de eigen email bestaat.

Samenhang met andere (toekomstige) ontwikkelingen

Het CBP maakt in algemene zin de kanttekening dat met de gefaseerde ontwikkeling van digitale voorzieningen en bijbehorende regelgeving, die uiteindelijk zal worden vastgelegd in de in voorbereiding zijnde Wet generieke digitale infrastructuur, het gevaar bestaat dat onvoldoende zicht is op, of onvoldoende rekening kan worden gehouden met, de samenhang tussen bepaalde voorzieningen en ontwikkelingen en de daarmee gepaard gaande risico's voor de bescherming van de persoon-lijke levenssfeer. Het CBP mist een overzicht van de samenhang in deze ontwikkelingen en een standpunt van de Minister en adviseert dit alsnog in de nota van toelichting op te nemen.

In reactie op het gestelde wordt opgemerkt dat het kabinet toewerkt naar betere publieke dienstverlening via het digitaal communiceren door en met de overheid en betere publieke dienstverlening. Dit is opgenomen in het Regeerakkoord 2012 en uitgewerkt in een Visiebrief (TK 26 643, nr. 280). Het onderhavige besluit maakt onderdeel uit van een groter geheel («Digitaal 2017») waar in stappen naartoe wordt gewerkt. Artikel X van de Wet EBV en de daarop gebaseerde uitvoeringsregelgeving, vormen de opmaat naar verdere regulering van de voorzieningen van de generieke digitale infrastructuur (GDI) die voor de realisering van Digitaal 2017 worden ingezet. Voor inzicht in de voorziene stappen, het tijdpad en de samenhang van de betrokken wetgevingstrajecten wordt verwezen naar de Kamerbrief «Uitgangspunten wetgeving generieke digitale infrastructuur» van 4 december 2015.[8] Anders dan het CBP lijkt te veronderstellen wegen de uitgangspunten van de Wbp voor de regering zwaar, en worden in de separate wetgevingsprocessen en feitelijke ontwikkelingen de relevante aspecten rondom de bescherming van de persoonlijke levenssfeer op tijd en in voldoende mate betrokken. Het onderhavige besluit vervult in dat verband een essentiële en robuuste functie.

Maatschappelijke noodzaak, «pressing social need»

Het CBP adviseert in de nota van toelichting (nader) te motiveren in hoeverre de inbreuk op de persoonlijke levenssfeer door de verplicht-stelling van het digitale berichtenverkeer met de Belastingdienst en het gebruik van de voorzieningen door betrokkenen wordt gerechtvaardigd

---

[8] Tweede Kamer 2015–2016 26 643 nr. 373.

door een «pressing social need». Het CBP constateert dat de omstandigheid, dat berichtenverkeer met de belastingplichtige verplicht op digitale wijze plaats moet vinden, (in beginsel) een inbreuk is op het recht op eerbiediging van de persoonlijke levenssfeer en stelt voorts dat de nota van toelichting daar ook vanuit gaat.

In reactie hierop zij opgemerkt, dat de nota van toelichting in paragraaf 8.2 stelt dat de verwerking van gegevens over een burger op zich een inbreuk vormt op diens persoonlijke levenssfeer, temeer daar de verwerking – gelet op het verplichte elektronische verkeer met de Belastingdienst – doorgaans niet op basis van vrijwilligheid plaatsvindt. Het gaat in het onderhavige besluit om de verwerking van persoonsgegevens in het kader van de voorzieningen, niet om de verplichting uit de Wet EBV tot verplicht digitaal berichtenverkeer met de Belastingdienst. De in paragraaf 8.2 van de nota van toelichting onder het kopje «Legitiem doel» gegeven onderbouwing van een dringende maatschappelijke behoefte moet in dat licht worden bezien. Het CBP stelt dat voor de toetsing aan artikel 8 EVRM van de verplichting in de Wet EBV en het besluit niet los van elkaar kunnen worden gezien. Echter, het besluit is niet de plaats om de dringende maatschappelijke behoefte van het verplichte elektronische verkeer met de Belastingdienst uit de Wet EBV te onderbouwen.

Hier wordt volstaan met een verwijzing naar de memorie van toelichting bij de Wet EBV, waarin nut en noodzaak van verplicht digitaal verkeer met de Belastingdienst uiteengezet worden.

Proportionaliteit: bewaartermijn en derdenverstrekking

Het CBP adviseert nader in te gaan op de noodzaak van de bewaartermijn voor gebruiksgegevens van 5 jaar, waarbij specifiek aandacht kan worden besteed aan de vraag hoe deze bewaartermijn zich verhoudt tot de overige in het ontwerp-Besluit opgenomen bewaartermijnen inzake andere gegevens dan gebruiksgegevens. Voor dat laatste verwijst het CBP naar een passage in de nota van toelichting over de bewaartermijn van 5 jaar in relatie tot misbruik en oneigenlijk gebruik.

In reactie daarop wordt het volgende opgemerkt. Het CBP beperkt de samenvatting van de in de nota van toelichting gegeven motivering voor de verlenging van de bewaartermijn van 5 jaar voor bepaalde gegevens tot de omstandigheid, dat het aantal gebruikers en de intensiteit van het gebruik is toegenomen en tot de toegenomen vraag van de burgers. De noodzaak voor de verlenging is echter meeromvattend. In paragraaf 6.3 van deze nota van toelichting is gewezen op het feit dat de voorzieningen steeds vaker een essentiële schakel vormen in de keten waarbij in de regel onderlinge contacten tussen burgers en afnemers voor langere tijd (veelal enige jaren) worden bewaard. Ook is aangegeven dat het gebruik van de voorzieningen direct van invloed kan zijn op de onderlinge rechten en verplichtingen. De wettelijke termijnen voor het afhandelen van aangiftes en toeslagen spelen ook een rol. Tenslotte is genoemd dat misbruik zich geregeld uitstrekt over een langere termijn dan de oude bewaartermijnen. Een langere bewaartermijn draagt dan bij aan adequatere ondersteuning en bescherming van burgers.

De passage over de bewaartermijn van 5 jaar die het CBP aanhaalt uit paragraaf 6.2 en op basis waarvan het CBP zich afvraagt, hoe de daar gebruikte formulering zich verhoudt tot de bewaartermijn voor bepaalde (en dus niet alle) gegevens van 5 jaar, heeft geen betrekking op de bewaartermijnen van gegevens in relatie tot misbruik en oneigenlijk gebruik, maar op de verwerking en verstrekking in het algemeen. Specifiek voor de bewaartermijnen wordt verwezen naar paragraaf 6.3.

Ook uit de formulering van de artikelen 11 tot en met 14 van het besluit blijkt duidelijk dat de bewaartermijn van 5 jaar niet voor alle gegevens geldt.

Bij het bepalen van de gegevens waarvoor een bewaartermijn van 5 jaar geldt, is uitgegaan van een inperking. Voor de categorie gebruiksgegevens is in de toelichting – zoals hierboven weergegeven – beargumenteerd dat deze voor een periode van 5 jaar dienen te worden bewaard. Hetzelfde geldt voor de actuele accountgegevens van DigiD en de gebruikersgegevens van DigiD Machtigen, waar de termijn van 5 jaar geldt vanaf het moment dat DigiD of DigiD Machtigen niet meer wordt gebruikt. Juist om privacyredenen is er voor gekozen om niet alle binnen de voorziening beschikbare gegevens voor een termijn van 5 jaar te bewaren, maar deze voor beheerdoelen te houden op 18 maanden en waar mogelijk nog (veel) korter. Dat laat echter onverlet – en daar heeft de zinsnede dat «niet op voorhand een beperking kan worden aangebracht in de gegevens die dienen te worden verwerkt en verstrekt» betrekking op – dat ook deze gegevens mogelijk dienen te worden verwerkt om misbruik effectief tegen te gaan. Zij worden echter voor dit doel niet langer bewaard.

Artikel 13 Wbp: beveiliging en de centrale rol van het BSN

Het CBP adviseert in de nota van toelichting expliciet aandacht te besteden aan de gevolgen van de verwerking van het BSN door verschillende partijen en stelt de vraag hoe de Minister van BZK een zorgvuldige verwerking door verschillende partijen verzekert.

In reactie op het gestelde is het van belang te benadrukken dat, anders dan het CBP meent, in deze nota van toelichting het BSN als een bijzonder persoonsgegeven in de zin van de Wbp wordt beschouwd, aan de verwerking waarvan extra strenge eisen worden gesteld. In dat verband zij opgemerkt dat afnemers van de GDI-voorzieningen als verantwoordelijke persoonsgegevens, waaronder het BSN, verwerken. Zij mogen dit in het kader van de uitoefening van hun publiekrechtelijke taak of op basis van specifieke wetgeving; op hen rust de verplichting aan de geldende eisen inzake onder meer (informatie)veiligheid te voldoen. Het is daarbij niet aan de Minister van BZK om, als verantwoordelijke voor de GDI, een zorgvuldige verwerking door de afnemers te verzekeren. Afnemers hebben immers een eigenstandige verantwoordelijkheid. Uitgangspunt voor de privacybescherming in Nederland is dat de verantwoordelijkheid voor de gegevensverwerking berust bij degene die de gegevens verwerkt en dat het toezicht daarop berust bij het CBP als de bij de wet aangewezen onafhankelijke toezichthouder.

Ook de Minister verwerkt persoonsgegevens, waaronder het BSN, te weten in de voorzieningen waarvoor hij een zorgplicht draagt. Voor wat betreft de gebruikersondersteuning met betrekking tot die voorzieningen geldt, dat hierbij moet worden onderscheiden tussen eerstelijns ondersteuning («klantcontactcentra») en tweedelijns ondersteuning («backoffice»). De eerstelijns ondersteuning geschiedt door een hiertoe gecontracteerde private partij; hiermee is namens de Minister van BZK als verantwoordelijke een bewerkerovereenkomst gesloten. In de bewerkersovereenkomst zijn onder meer bepalingen opgenomen over de verplichtingen van de opdrachtnemer inzake het verwerken van persoonsgegevens en de beveiliging hiervan. De tweedelijns ondersteuning maakt deel uit van de beheerstaak met betrekking tot de voorzieningen. Hiervoor is de Minister van BZK verantwoordelijk en moet hij voldoen aan de bepalingen inzake de bescherming van persoonsgegevens in het onderhavige Besluit en aan de beveiligingsmaatregelen die gelden ingevolge de Regeling voorzieningen GDI. Voor wat betreft de voorziening

BSN-koppelregister worden door de Minister van BZK als verantwoordelijke bewerkersovereenkomsten gesloten met private partijen (ook wel authenticatiediensten genoemd) die authenticatiemiddelen willen aanbieden voor gebruik in het publieke domein. Hierop wordt nader ingegaan onder 10.1.7.

Gelet op het bovenstaande is paragraaf 6.1 van de nota van toelichting aangevuld.

Het CBP adviseert voorts om in de nota van toelichting de inrichting van de beveiliging van de voorzieningen, in het licht van de Regeling voorzieningen generieke digitale infrastructuur, uiteen te zetten, alsmede zo nodig aan te passen en/of te concretiseren.

In reactie hierop zij opgemerkt, dat de beveiliging van de voorzieningen niet wordt geregeld in het onderhavige besluit. Daartoe dient, zoals het CBP zelf ook opmerkt, de Regeling voorzieningen GDI. De in de regeling genoemde maatregelen zien onder meer op te hanteren informatietechnologie, beveiligingstechnieken, (normalisatie)normen en standaarden en managementsystemen voor informatiebeveiliging. Het zou te ver voeren om de inrichting van de beveiliging van de voorzieningen in het kader van dit besluit verder uiteen te zetten.

Subsidiariteit

Het CBP adviseert, in reactie op het in de nota van toelichting gestelde dat het ontwerp-Besluit de bestaande praktijk bij de voorzieningen vastlegt en dat niet is bekeken of een andere wijze dan de bestaande voorzieningen mogelijk minder ingrijpend zou zijn, om in de nota van toelichting het antwoord op de vraag naar de subsidiariteit met betrekking tot de verplichte gegevensverwerking zoals opgenomen in de Wet EBV (alsnog) onder ogen te zien en te onderbouwen.

In reactie op het door het CBP gestelde wordt opgemerkt dat, zoals in paragraaf 8.2 is aangegeven, het besluit primair de gegevensverwerking vastlegt van reeds bestaande en sinds jaar en dag door de overheid en burgers gebruikte voorzieningen. Het in dat kader volledig heroverwegen van het nut en de noodzaak van die voorzieningen zou niet reëel en niet opportuun zijn. Of in het kader van het verplichte elektronische verkeer met de Belastingdienst in de Wet EBV voor een andere voorziening gekozen had kunnen worden dan waarin de beschikbare generieke digitale infrastructuur voorziet, te weten de diensten van de Berichtenbox van de voorziening MijnOverheid, is een subsidiariteitsvraag die niet thuishoort in de nota van toelichting bij dit besluit. Kortheidshalve zij verwezen naar de memorie van toelichting bij de Wet, in het bijzonder paragraaf 2.2 daarvan.[9]

Het BSN-Koppelregister

Het CBP adviseert de Minister om te motiveren waar, onder verwijzing naar passages in de nota van toelichting, in het samenstel van bepalingen de verankering van het gebruik van het BSN door private partijen is geregeld en hoe dit zich verhoudt tot het uitgangspunt uit de nota van toelichting dat voor de verwerking van het BSN bewerkersovereenkomsten dienen te worden gesloten (hetgeen op zichzelf volgens het CBP terecht suggereert dat er geen wettelijke grondslag is voor private partijen om het BSN te verwerken).

---

[9] Tweede Kamer 2014–2015 34 196 nr. 3.

In reactie op het gestelde wordt opgemerkt dat voor het goed functioneren van de voorzieningen voor de generieke digitale infrastructuur, en dus ook het BSN-Koppelregister (met als taak: identiteitsverificatie), artikel X, derde lid, van de Wet EBV in een expliciete wettelijke grondslag voor de verwerking van persoonsgegevens voorziet, waaronder het BSN, door de Minister van BZK. Als beheerder van de GDI en verantwoordelijke voor de verwerking van persoonsgegevens is hij vervolgens gerechtigd een bewerker in te schakelen. De verwerking van het BSN door het BSN-koppelregister ten behoeve van de authenticatie met een privaat middel in het publieke domein vindt dus haar wettelijke basis in artikel X van de Wet EBV. Oftewel, artikel X van de Wet EBV biedt aan private partijen (authenticatiediensten) de basis om het BSN te verstrekken in de hoedanigheid van *bewerker* voor de Minister van BZK als verantwoordelijke en beheerder van het BSN-Koppelregister. In de bewerkersovereenkomst wordt onder meer opgenomen dat de verwerking van het BSN gebonden is aan strikte regels en het BSN ingevolge artikel 24, eerste lid, van de Wbp slechts zal worden verwerkt voor doeleinden bij de wet bepaald, dat de bewerkersovereenkomst slechts ziet op de verwerking van het BSN in het kader van de doorgifte aan het BSN-Koppelregister en dat na aanlevering het BSN niet mag worden bewaard.

Gelet op het bovenstaande is paragraaf 7.2 van de nota van toelichting aangevuld.

10.2 Internetconsultatie

In de internetconsultatie is een zorg geuit over de beveiliging van de voorzieningen, meer specifiek over de (on)mogelijkheden tot afluisteren. In reactie daarop kan worden gemeld dat de beveiliging van de voorzieningen zeer serieus wordt genomen. De rijksbrede en overige normen die daarvoor gelden staan in de Regeling voorzieningen GDI, die eveneens hoort bij de Wet EBV. Deze regeling was nog niet gepubliceerd ten tijde van de internetconsultatie. De servers van de betrokken voorzieningen staan in Nederland en de data wordt door alle betrokken leveranciers uitsluitend binnen de Europese Unie verwerkt. Derhalve is daarop het EU-privacyregime van toepassing. Dit is tevens conform het beleid van de Nederlandse overheid ten aanzien van cybersecurity, de bescherming van de belangen van veiligheid, beschikbaarheid en integriteit in relatie tot dreigingen op het internet in algemene zin. Ook is opgemerkt dat het erop lijkt dat de voorzieningen het karakter hebben van «Big Brother is Watching You». In reactie daarop kan worden gemeld dat, anders dan de geuite zorg, dit besluit bedoeld is om duidelijkheid te geven over de noodzakelijke verwerking van persoonsgegevens door de voorzieningen en de doelen waarvoor dat gebeurt. DigiD is en blijft – dit besluit brengt daarin geen verandering – het veilige hulpmiddel voor authenticatie dat burgers ten dienste staat om in te loggen bij overheidsorganisaties of organisaties met een wettelijke taak. Gegevens waartoe de burger toegang krijgt bij de afnemer na succesvol inloggen met DigiD als digitale sleutel worden niet opgeslagen door DigiD.

Artikelsgewijs

Artikel 1

De omschrijving van een deel van de in artikel 1 opgenomen begrippen spreekt voor zichzelf. Een aantal begrippen wordt hieronder nader toegelicht.

Gebruiker

Voor de omschrijvingen van het begrip gebruiker is allereerst aangesloten bij de oude gebruiksvoorwaarden van DigiD en MijnOverheid. Een gebruiker moet ingeschreven zijn in de BRP, als ingezetene of als niet-ingezetene, aangezien iemand alleen dan over een BSN beschikt en dat nummer is essentieel voor de werking van de voorzieningen DigiD, DigiD Machtigen en MijnOverheid.

Voor DigiD is pas sprake van een gebruiker als het digitale aanvraagproces met succes is afgerond, in de praktijk zodra hij op de website de mededeling krijgt dat de aanvraag is gelukt en dat de brief met de activeringscode zal worden verzonden. Zie het algemeen deel van deze nota van toelichting voor een meer uitgebreide beschrijving van de procedure. De eerdere tussenstap waarbij de gebruiksvoorwaarden moesten worden geaccepteerd, is niet meer nodig nu de verwerking van persoonsgegevens is gebaseerd op de publiekrechtelijke taak van de Minister van BZK in artikel X van de Wet EBV (artikel 8, onderdeel e, van de Wet bescherming persoonsgegevens).

Voor MijnOverheid is sprake van een gebruiker zodra een account is aangemaakt. Dat gebeurt, zoals hiervoor is uiteengezet, ambtshalve door de Minister van BZK. Zie hiervoor hoofdstuk 5 van het algemeen deel van deze nota van toelichting. Het vereiste uit de oude gebruiksvoorwaarden van MijnOverheid dat een gebruiker in het bezit moet zijn van een DigiD is om die reden vervallen; immers, degene ten behoeve van wie een account wordt klaargezet, hoeft op dat moment nog niet over een DigiD te beschikken.

Gemachtigde

Aangezien een gemachtigde, anders dan een vertegenwoordigde, altijd moet beschikken over een DigiD, is in de beschrijving van het begrip gemachtigde expliciet verwerkt dat deze een gebruiker van DigiD moet zijn.

Overheidsorgaan en afnemer

In dit besluit is ervoor gekozen om voor de omschrijving van het begrip afnemer te verwijzen naar het begrip overheidsorgaan, zoals dat is geformuleerd in de Wet algemene bepalingen burgerservicenummer (Wabb) en ook is gebruikt in de Archiefwet 1995 en de Wet basisregistratie personen. Het begrip overheidsorgaan is in de Wabb op dezelfde wijze omschreven als het begrip bestuursorgaan in de Algemene wet bestuursrecht (Awb). Echter, op grond van artikel 1:1, tweede lid, van de Awb worden bepaalde organen, personen en colleges, zoals de Nationale ombudsman, de Eerste en Tweede Kamer, de Algemene Rekenkamer en gerechtelijke instanties, niet als bestuursorgaan aangemerkt. Door het gebruik van het begrip overheidsorgaan zoals bedoeld in de Wabb wordt de reikwijdte van de omschrijving verruimd, doordat de in de Awb niet als bestuursorgaan aangemerkte organen, personen en colleges wel onder het begrip overheidsorgaan vallen. Die bredere reikwijdte sluit ook beter aan bij de ruime formulering in de oude gebruiksvoorwaarden en is ook nodig, omdat de in de Awb uitgesloten organen (bijvoorbeeld gerechtelijke instanties) mogelijk in de toekomst ook gebruik zullen willen maken van DigiD, DigiD Machtigen en MijnOverheid.

Naast overheidsorganen vallen onder het begrip afnemer ook organisaties of rechtspersonen, die geen bestuursorganen zijn, maar wel een wettelijke taak hebben, zoals zorgverzekeraars, academische ziekenhuizen en onderwijsinstellingen. Daarmee is de reikwijdte identiek aan die van de oude gebruiksvoorwaarden.

De groep afnemers is, in lijn met de eerdere gebruiksvoorwaarden, ook beperkt tot die organisaties die voor de uitoefening van hun publieke taak of bevoegdheid gebruik maken van een afnemersdienst en bij het aanbieden daarvan gebruik maken van DigiD, DigiD Machtigen respectievelijk gebruik maken van MijnOverheid. Dat het bij het gebruik van MijnOverheid moet gaan om organisaties die elektronisch verkeer met andere overheden en burgers wenselijk achten keert in de omschrijving in dit besluit niet terug, aangezien dit criterium in de andere criteria volgt.

Artikelen 2 tot en met 4

In deze artikelen zijn de persoonsgegevens opgenomen die worden verwerkt in het kader van de voorzieningen DigiD, DigiD Machtigen en MijnOverheid. Overigens is het niet zo dat al deze gegevens die in het algemeen worden verwerkt in het kader van de voorzieningen, ook van alle individuele gebruikers van de voorzieningen worden verwerkt. Zoals blijkt uit de beschrijvingen in de hoofdstukken 3, 4 en 5, is de verwerking van bepaalde gegevens afhankelijk is van de wens of de situatie van de gebruiker zelf (zo moet bij zijn e-mailadres opgeven als hij gebruik wil maken van de wachtwoordherstelfunctie van DigiD) of van de gebruikte aanvraagprocedure (het nummer van het Nederlandse paspoort of de Nederlandse identiteitskaart wordt enkel gebruikt bij de aanvraagprocedure aan de balie buitenland).

Met de aanduiding «naam en de noodzakelijke gegevens om deze correct weer te geven» wordt bedoeld dat het bij het gegeven naam meer in detail gaat om de voornamen en achternaam, eventuele predicaten of adellijke titels en informatie over het naamgebruik van gehuwden, inclusief de daarvoor noodzakelijke informatie over de naam van de huwelijkspartner. Het adres omvat (uiteraard) ook de woonplaats.

In de artikelen 3, onderdeel b, onder 5°, en 4, onderdeel b, onder 5°, is verder, in lijn met DigiD, ook voor DigiD Machtigen respectievelijk MijnOverheid bepaald dat gegevens kunnen worden verwerkt die relevant zijn voor de adequate werking van de voorziening. Dat is onder meer nodig omdat de website van DigiD Machtigen geschikt wordt gemaakt en de website van MijnOverheid geschikt is voor mobiele apparaten waarvoor het nodig kan zijn om het type browser uit te vragen.

Artikel 10

Het is in verband met de bescherming van de persoonlijke levenssfeer van belang om de verstrekking van gegevens die over bezoekers en gebruikers bekend zijn bij de Minister van BZK, voor zover niet gereguleerd in de artikelen 6 tot en met 9, in te perken. In dit artikel is daarom bepaald dat verstrekking van gegevens aan anderen dan de bezoeker of de gebruiker zelf (in het kader van bijvoorbeeld hun recht op inzage) slechts mogelijk is als zij daartoe toestemming hebben gegeven. In twee gevallen is die toestemming niet nodig.

Ten eerste is geen toestemming nodig indien het gaat om het verstrekken van gegevens aan overheidsorganen of rechtspersonen me een wettelijke taak die bijvoorbeeld behulpzaam kunnen zijn in de constatering of bij bepaalde door de Minister van BZK opgemerkte signalen inderdaad sprake is van misbruik of oneigenlijk gebruik van de voorzieningen, mits dat verstrekken noodzakelijk is voor de borging van de beveiliging en betrouwbaarheid van de betreffende voorziening (onderdeel a). Dit is mede in het belang van de rechtmatige houder van een DigiD, een machtiging of een MijnOverheid-account in die gevallen waarin hij schade ondervindt als gevolg van misbruik of oneigenlijk

gebruik ervan door een ander (zie verder paragraaf 6.2 van het algemeen deel van deze nota van toelichting).

Ten tweede is geen toestemming nodig indien de Minister van BZK op grond van andere wettelijke bepalingen gerechtigd is tot verstrekking van bepaalde gegevens over te gaan.

Zie over artikel 10 ook paragaaf 8.4 van het algemeen deel van deze nota van toelichting.

Artikel 11

In het vierde lid is tot uitdrukking gebracht dat het BSN in ieder geval gedurende het aanvraagproces wordt bewaard. Als het DigiD daarna ook wordt geactiveerd, wordt het bijbehorende DigiD bewaard zo lang het geldig is, tot 5 jaar na het moment waarop dat niet meer zo is. Alleen als een aangevraagd DigiD niet wordt geactiveerd, verloopt de bewaartermijn van het BSN na maximaal 18 maanden in de reguliere procedure. Bij de balieprocedure is in dat geval slechts een termijn van 6 maanden nodig. Zie verder hoofdstuk 3 van het algemeen deel van deze nota van toelichting.

Artikel 16

Het moment van inwerkingtreding van dit besluit hangt samen met de inwerkingtreding van artikel X van de Wet EBV op 1 november 2015 en de in het derde lid van artikel X van deze wet geformuleerde opdracht tot het stellen van nadere regels voor de verwerking van persoonsgegevens in de betreffende GDI-voorzieningen. Om redenen van rechtszekerheid en zorgvuldigheid is aan het besluit terugwerkende kracht verleend. Dit heeft geen benadeling van burgers tot gevolg. Voor de inwerkingtreding is aldus, gelet op het spoedeisende karakter, afgeweken van het beleid voor Vaste Verander Momenten.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk